Keith Cook Training Limited

Policies and Procedures

Relevant to:

All Training including CPCS testing, AITT, NPORS, BALI/ROLO & Lantra Awards Accrediting Bodies.

CITB SQA & NOCN Awarding Body

Version 1.6.0 dated 05/01/2026

Work-Based Learning and Assessment for Adult Apprenticeships and NVQ/QCF/NWSWA in line with Pearson & SQA Awarding Bodies

.

Position	Name	Signature	Reviewed Date
Manager	George Walton Cert IOSH		05 January 2026
Director	James Cook MD		05 January 2026

Note:

All candidates who are employed and working on their employer's premises during the training and/or assessment period will be expected to know, understand, and follow their own company's policies and procedures.

Should a conflict arise in the content of a Keith Cook Training Limited policy and one from the candidate's own employer, the employer's policy and/or procedure will take precedence.

The policies and procedures contained in this document relate to candidates, trainee's visitors, and learners whilst on Keith Cook Training Limited premises.

Keith Cook Training Limited staff and representatives are expected to adhere to the appropriate KCTL procedures when on KCTL business at any location.

INDEX	
Part 1 General Policy Statement	4
Part 2 Organisation	5
KCT Ltd Organisational Chart	5
Part 3 Responsibilities	6
Health and Safety Director	6
Health and Safety (on/off site)	6
Health and Safety (Office)	7
Employees, Registered Instructors, Assessors, Internal Verifiers, Sub-Contractors, and Agents	7
Information Advice & Guidance	7
Part 4 General Arrangements	8
Management of Health and Safety	8
Health and Safety Training	8
Incident Reporting	8
Fire, Evacuation and Emergencies (FEEP)	8
Discovery of Explosives, Suspicious Packages etc on Client's Premises	9
Substances Hazardous to Health (COSHH)	9
Work Equipment	10
Personal Protective Equipment (PPE)	11
Manual Handling	11
Grievance Procedure	19
CCTV	24
Part 5 Safety Rules for Contractors, Registered Instructors, Assessors and Internal Verifiers	25
Alcohol and Drugs	25
Smoking	23
Accident Reporting Procedure	26
Accident Investigations	26
Equal Opportunities Policy	25
Prevention of Discrimination Policy	26
Children and Vulnerable Adults Policy	28
Lone Worker Policy	29
Data Protection Policy	30
Use of Computers and Communication Systems	37
Environmental Policy	41
Quality Policy	41
Equality and Diversity Policy	42
Customer Service Policy	43

Customer Complaints Procedure	43
Conflict of Interest Policy	44
Appeals (Training & CPCS Testing)	44
Appeals (NVQ/QCF/Adult Apprenticeships)	45
Whistle Blowing	46
Refuelling Procedures	46
Part 6 – Appendices & Awarding/Accrediting Bodies additional requirements	48
Part 7 – Procedures & templates	74
Current Staff	74
Site Specific Risk Assessment	75
KCTL Fire Risk Assessment	77
Remedial Action Plan for KCT Ltd	92
Fire Evacuation Plan Map with Fire Call and First Aid Points	96
Part 8 Safeguarding Adults Policy Statement Including Prevent	99
Policies On Slavery and Human Trafficking (Modern Slavery Act 2015)	99
Prevention and Awareness Raising	100
Part 9 – Decision Planning Strategy Plans with Policy Outcomes	110
Decision and Strategy Stage 1	110
Strategy and Protection Plan Stage 2	111
Policies in place from Stage 1 & 2	112
The Centre Environment	112
Education for Sustainable Development	113
Working with the Community	114
Animal Welfare	115
Malpractice & Maladministration Policy	117
Recognition of Prior Learning (RPL)	119
Conflict of Interest policy	120
Part 10 Information Security Policy For Card Payments	122
Part 11 SQA Streetworks - Certificate release	146

Part 12 Additional Policies and Information for Awarding and Accrediting Bodies	152
KCT CPCS IQA Policy	152
KCT – Coronavirus Policy (For Advise Only)	154
KCT Booking Process Overview	158
KCT IQA PROCESSING	159
KCT Company Vehicle Accident Procedure	166
INFECTIOUS DISEASE OR VIRUS PANDEMIC	167
KCT CITB ITC & SSP Policy & Procedure	169
Reasonable Adjustment Policy	173
CITB SSP Exam Procedures	178
CITB Approved Training Organisation Procedures	180
CITB SSP Examination Requirements	181
CITB Trainer Approval	182
Use a Defibrillator	182
CITB Fair Notice Form	183

Health and Safety Policy and Procedure

Part 1 - General Policy Statement

Keith Cook Training Limited acknowledges and accepts its statutory responsibilities, in the terms of the Health and Safety at Work Act 1974, and the Management of the Health and Safety at Work Regulations 1998 and other relevant legislation, for securing the health, safety and welfare of all its employees, registered instructors, assessors, internal verifiers, sub-contractors or agents, where statutory duties exist.

Keith Cook Training Limited will take all reasonable steps within its power to meet this responsibility, paying particular attention to the provision and maintenance of: -

- Plant, equipment, and systems of work that are safe
- Safe arrangements for the use handling and transportation of articles and substances
- Sufficient information, instruction, training, and supervision to enable all employees, registered instructors, sub-contractors, or agents to avoid hazards and to contribute positively to their own health and safety at work.
- A safe place of work with safe access and egress
- Adequate welfare facilities
- Information on general health issues

The success of any safety policy in reducing accidents depends ultimately on the good sense and safety consciousness of everyone at work. Keith Cook Training Limited expects all employees, registered instructors, assessors, internal verifiers, sub-contractors, or agents to recognise their own responsibilities with regard to their own health and safety and that of other people, and to co-operate with Keith Cook Training Limited so as to enable it to carry out its own responsibilities successfully.

This statement must be read in conjunction with the further statements on:-

Part 2 Organisation
Part 3 Responsibilities
Part 4 General Arrangements
Part 5 Safety rules for registered instructors, assessors, internal verifiers, sub-contractors, or agents.
Part 6 Risk Assessments & Action Plans

A copy of this document will be made available to all employees, registered instructors, assessors, internal verifiers, sub-contractors, or agents. It may be reviewed or amended periodically and may be supplemented, as appropriate by further statements relating to particular works.

Part 2 – Organisation

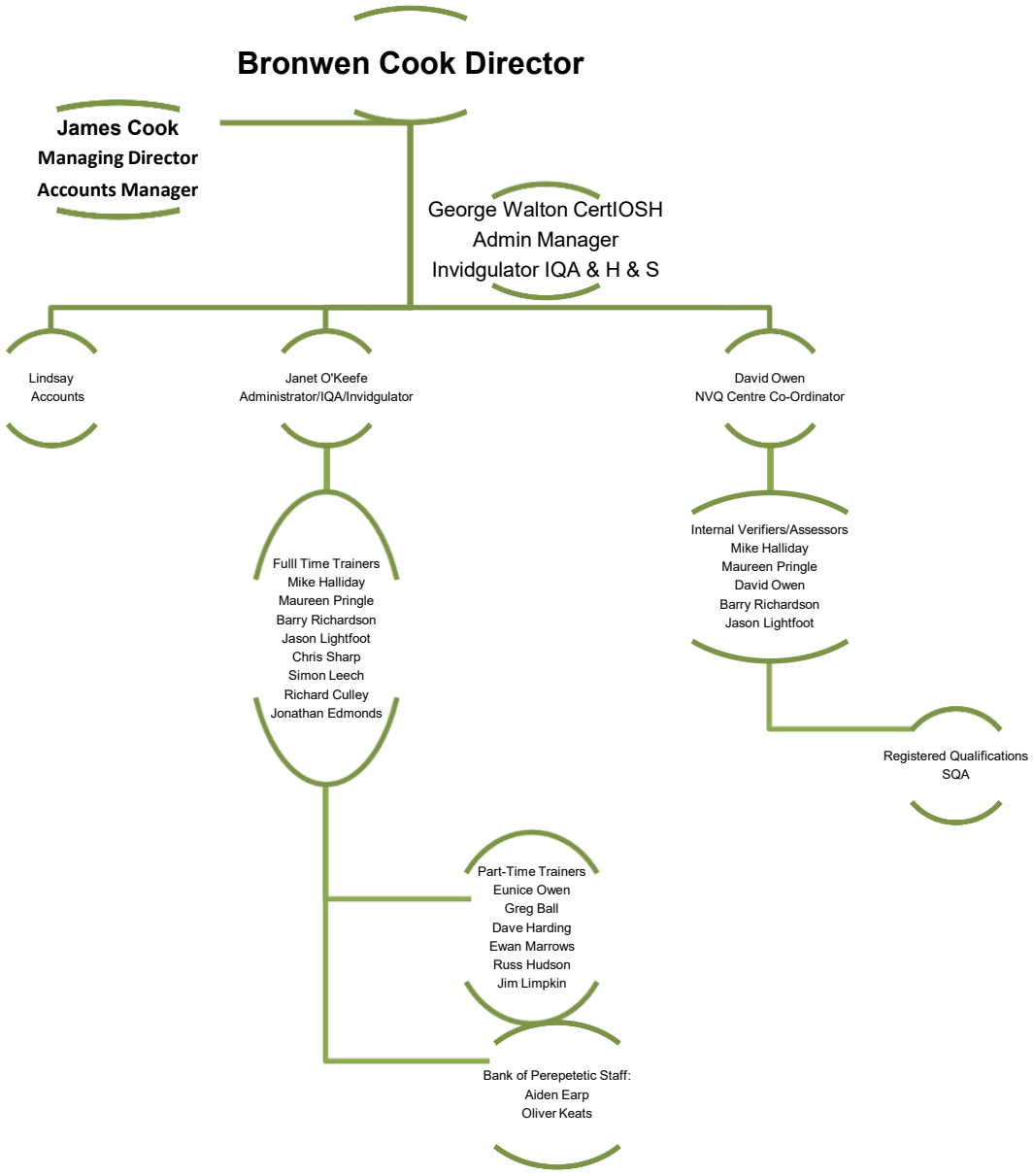
The organisation of responsibility for all matters related to Health and Safety within Keith Cook Training Limited will be through the management structure as follows: -

Health and Safety Director – James Cook

Office Health and Safety & Off Site - George Walton CertIOSH

Health and Safety on Site - Michael Halliday

Organisational Chart



Part 3 – Responsibilities

Health and Safety Director, James Cook - Advisor George Walton CertIOSH

The health and safety director are responsible for notifying changes in statutory and Keith Cook Training Limited requirements in health and safety matters. He will:-

(a) Maintain a constant awareness of any changes in Health and Safety Legislation

(b) Formulate Keith Cook Training Limited Health and Safety Policy and liaise with the relevant health and safety authorities as required.

(c) Provide pertinent and meaningful guidelines and advice on health and safety problems or matters arising.

(d) Ensure that Keith Cook Training Limited Health and Safety Policy Document and any appropriate guidance documents are made available to every employee, registered instructor, assessor, internal verifier, sub-contractor, or agent.

(e) Arrange training for all as required.

(f) Carry out Safety Audits at regular intervals, and subsequently advise as appropriate.

(g) Investigate and report on all serious accidents.

(h) Ensure all necessary assessments are completed and reviewed.

(i) Set a personal example by demonstrating high standards of application and discipline in Health and Safety

Health and Safety (on site/off site), Michael Halliday - Advisor George Walton CertIOSH

(a) Develop safe working practices and maintain a high standard of cleanliness.

(b) Ensure that all safety rules are observed and inspect methods, operations, and premises, both existing and new, to ensure compliance with Keith Cook Training Limited Safety Policy. Offsite assessing, training, or testing this information must be collected at the time of booking and any information issued to the instructor/assessor/trainer 24 hours before attendance, they should also be made aware of any site induction requirements in accordance with the offsite policies and procedures for the customers site, refer to the terms and conditions relevant to the awarding/accrediting bodies.

(c) Report to the Health and Safety Director all accident and/or incidents to persons, plant or equipment, fires, property damage and occupational illness and ensure their adequate recording.

(d) Investigate the above to ascertain causes and take appropriate remedial action to prevent recurrence.

(e) Instruct employees, registered instructors, assessors, internal verifiers, sub-contractors, trainees, delegates, candidates, visitors, and agents about any hazards associated with their work and any necessary precautions required.

(f) Ensure all employees, registered instructors and agents are properly trained.

(g) Ensure (off site only) customer's policies & procedures are followed.

Health and Safety (Head Office), George Walton CertIOSH

(a) Develop safe office working practices and maintain a high standard of cleanliness.

(b) Ensure that all office safety rules are observed, and to inspect all office premises, both existing and new, to ensure compliance with Keith Cook Training Limited Safety Policy.

(c) Report to the health and Safety Director all accidents and/or incidents to persons, office equipment, fires, property damage and occupational illness and ensure their adequate recording.

(d) Investigate the above to ascertain causes and take appropriate remedial action to prevent recurrence.

(e) Instruct office staff about any hazards associated with their work and any necessary precautions required, including evacuation procedures in the event of fire, accident, or incident.

(f) Ensure all office staff are properly trained.

(g) Ensure all visitors to Head Office are informed of Keith Cook Training Limited safety requirements, including evacuation procedures in the event of fire, accident, or incident.

Employees, Registered Instructors, Assessors, Internal Verifiers, Sub-Contractors and Agents

It is the duty of all employees, registered instructors, assessors, internal verifiers, sub-contractors or agents to exercise personal responsibility to prevent injury or danger to themselves or to others and they must: -

(a) Co-operate with Keith Cook Training Limited in preventing accidents and/or health risks.

(b) Comply with Keith Cook Training Limited and their clients' Health and Safety Policy and any associated policies and procedures.

(c) Wear and use personal protective equipment as instructed or when circumstances dictate its use.

(d) Report **all** accidents and injuries, no matter how trivial and any dangerous occurrences or near misses.

Information Advice & Guidance

IAG Aim
KCTL aims to provide impartial and robust information, advice and guidance to all learners and potential learners to enable them to achieve individual goals and to improve skills, qualifications, and employment prospects.
IAG Objectives
-To ensure all learners are informed of and understand what to expect from a KCTL programme of learning
-To provide all learners with an accessible information, advice and guidance service that is impartial, objective, and confidential
-To provide a service that promotes equality and diversity and is free from discrimination and to measure equality and diversity impact measures (EDIMs)
-To provide information, advice and guidance that is flexible in meeting the needs through a tailored service and effective signposting and referral process
-To maximise success and retention rates amongst all learners by supporting individual needs and objectives
-To maximise career and learning progression
-Where possible, to move learners towards sustained employment
-To ensure the information, advice and guidance service is evaluated by learners, partners and staff on a regular basis and this feedback leads to continuous improvement in the service

Part 4 - General Arrangements

It is the legal duty of all management, supervision, employees, registered instructors, assessors, internal verifiers, sub-contractors, and agents to do everything to prevent accidents, personal injury and danger to themselves, other employees, or members of the public.

Management of Health and Safety

Risk assessments will be undertaken, as necessary, to assess where risks may arise and to ensure all measures are taken to control such risks.

Employees, registered instructors, assessors, internal verifiers, sub-contractors, and agent will be informed of the outcome of such risk assessments and the preventative and protective measures required.

Regular health and safety monitoring audits and inspections will be undertaken to review control measures.

Health and Safety Training

Employees, registered instructors, assessors, internal verifiers, sub-contractors, and agency personnel will receive safety training, such training should ensure that they are aware of their health and safety responsibilities and are competent to operate any plant, tools, equipment, and vehicles as required.

Incident Reporting

All accidents, no matter how trivial, must be recorded in the accident book.

Minor Accidents

- To be treated, if possible, by a qualified First Aider.
- Note detail in the accident book.
- Inform a responsible person.

Major Accidents

- Where appropriate give First Aid, by a qualified person
- Inform Emergency Services immediately (ambulance, fire and rescue service)
- Inform a responsible person immediately (site agent, supervisor or similar)

Fire, Evacuation and Emergencies

It is the duty of all employees, registered instructors, assessors, internal verifiers, sub-contractors, and agents to familiarise themselves with the fire and emergency evacuation procedures in force at the premises where they are working. If in doubt they must request the information from the designated contact within the organisation. Every employee, registered instructor, sub-contractor, and agent must ensure that any visitors or trainees under their responsibility are safely evacuated and are accounted for. See Annex A KCT Ltd Fire Risk Assessment.

Fire Emergency Evacuation Plan (FEEP)

1. **Action on discovering a fire**, it is the duty of every person to sound the nearest fire alarm immediately. All call points are displayed on notice boards at the centre and all visitors/trainees are made aware of this during their induction.

2. **Action on hearing the fire alarm** KCT Ltd staff should precede to the pre-determined positions to assist visitors/trainees/staff to leave the building by the nearest safe route. Personnel should not re-enter the building until notified by the Fire Warden or Emergency Services.

3. **Calling the Fire Brigade**, this is to be done immediately by the main office or person discovering the fire. The number from the main land line is 999.

4. Fire Fighting Equipment All staff are trained in the use of firefighting equipment, however any fire that is larger than a wastepaper bin in size should be left to the fire brigade, under no circumstances should you put yourself or any person at risk.

5. **Power Isolation** Electricity can be cut to the whole site from the generator house, the Fire Warden will inform the Fire Brigade on arrival.

6. **Identification of Escape Routes** All escape routes are clearly marked and displayed throughout the centre.

7. **Fire Wardens** All KCT Ltd key staff have been trained in the use of fire extinguishers and certified in the use of. The site buildings are all at ground level with the exception of one classroom and so does not require a complex evacuation procedure.

8. **Fire Drills** are carried out on a regular basis which ensures all personnel know the alarm points, primary and secondary escape routes, and close down procedures. Records are kept in the main office of all Fire Checks.

9. **Personal Emergency Evacuation Plan (PEEP)** Because of the nature of this business there is no requirement at this time for this action.

10. **Liaison with Emergency Services** the fire warden will provide information of the site to the fire and rescue service which will include a site plan; any must include details of the roll call confirming that everyone has exited the buildings.

Discovery of Explosives, Suspicious Packages etc on Client's Premises

Do not touch any suspicious items.

Inform the client's site security who should immediately arrange evacuation of the area and contact the emergency services.

Before leaving take all necessary precautions so that nobody, even mistakenly, can come into contact with the object before the arrival of the emergency services.

Substances Hazardous to Health (COSHH)

It is the responsibility of the Health and Safety Director to ensure that all substances are supported with adequate information and instructions for use. The Health and Safety director must ensure that all employees, registered instructors, sub-contractors, and agents are instructed, informed, and trained in using such substances before use and, where necessary make arrangements for adequate supervision.

Precautions When Using Substances

The following precautions should be taken by all employees, registered instructors, assessors, internal verifiers, sub-contractors, and agents.

Ensure familiarity of rules governing the use of hazardous substances

Handle hazardous substances with care and in accordance with instructions on the hazardous material information sheet.

Use such personal protective equipment as is necessary and appropriate.

After handling hazardous substances, ensure that hands are thoroughly washed before eating, drinking or smoking.

In the event of a spillage or contamination, the nature of the substance and its source should be established, then the correct procedure followed as outlined on the hazardous material information sheet.

Work Equipment

Keith Cook Training Limited will take all reasonable steps to meet the requirements of the Provision and Use of Equipment Regulations, and any other relevant legislation, particularly with regards to performance standards of equipment and statutory inspections.

Records of plant/equipment wholly owned by Keith Cook Training Limited will be compiled and maintained for the purpose of planned, preventative maintenance in accordance with current legislation.

Where Keith Cook Training Limited employees, registered instructor's assessors, internal verifiers, sub-contractors and agents are likely to be exposed to potentially hazardous situations, through plant and/or equipment not in the ownership of Keith Cook Training Limited, such matters must be brought to the notice of those responsible for such equipment. Such plant and/or equipment must not be used until all faults have been rectified.

Before using any work equipment, all employees, registered instructors, assessors, internal verifiers, sub-contractors and agents must: -

- Ensure they are authorised to use it and be familiar with the manufacturers operating instructions, prior to use.
- Be familiar with manufacturers' safety instructions prior to use.
- Report, immediately, any sign of irregular operation
- Check all electrically powered items of equipment for signs of damage, i.e. cables and plugs.
- Check all portable electrically powered items they are to use have been tested and show a pass label.
- Check all guards are secure and correctly fitted prior to use.

Personal Protective Equipment

All Keith Cook Training Limited employees, registered instructors, assessors, internal verifiers, sub-contractors, and agents must wear/use personal protective equipment as and when appropriate.

Manual Handling

Keith Cook Training Limited will take all reasonable steps to meet the requirements under the Manual Handling Operations Regulations, 1992, including: -

- The analysis of all manual handling activities to assess risk and take appropriate measures to avoid or reduce such risks to the lowest levels reasonably practicable.

- Provide suitable and sufficient information, instruction, and training (and where necessary supervision) to control any risks that cannot be eliminated by other means.

SICKNESS ABSENCE POLICY, PROCEDURES AND GUIDELINES

KEITH COOK TRAINING LTD (the employer) Attendance Management Policy

1. Introduction and purpose

1.1 This policy is designed to improve employee attendance by ensuring that issues to do with employee health and wellbeing are addressed in an appropriate and timely manner. It outlines the processes the employer will follow in cases where an employee's attendance is a cause for concern.

1.2 This policy applies to all employees except that sections 10-12 and 14 will not apply to those serving a period of probation. Concerns about attendance for employees on probation will be considered as a factor in the review of the probationary period and in accordance with the probation policy: Support, Review and Guidance Procedure for Employees Serving a Probationary Period.

1.3 This policy does not form part of any contract of employment and may be amended at any time.

2. Guiding principles

The policy is underpinned by the following guiding principles:

i. good attendance is valued, and the employer will put appropriate mechanisms in place to support employee attendance.

ii. All sickness absence is presumed to be genuine, and matters raised relating to an employee's attendance do not imply any distrust of staff or concerns regarding their conduct.

iii. Employee absence will be dealt with in a way that is non-discriminatory and in accordance with the employer's commitment to equality.

iv. A degree of employee absence is inevitable but there may be occasions where an employee's overall attendance levels are a cause of concern.

3 Roles and responsibilities

3.1 The employer is responsible for managing attendance and is expected to intervene early to attempt to secure an improvement in employee attendance where it does not reach the standards expected.

3.2 Managing attendance is about managing people on an individual basis. The employer will keep in touch with absent employees on a regular basis to ensure that contact with the employer is maintained and to help facilitate the employee's early return to work.

3.3 The employer is responsible for conducting risk assessments where necessary and keeping them under review to reduce the level of risk and help to maintain health and wellbeing at work.

3.4 The employer is responsible for ensuring employee absence is accurately recorded on its absence management system and is accountable for keeping this up to date.

4. Employees

4.1 All employees are required to carry out their duties unless not fit to do so and comply with the employer's absence reporting and attendance procedures.

4.2 Employees should raise concerns if they believe that their job is making them ill or

contributing to illness and co-operate fully with Occupational Health and other organisations that provide support.

5. Services and support for managing attendance

5.1 The Occupational Health Service and the Government 'Fit for Work' scheme provide a range of services to assist the employer in taking a proactive approach to attendance. Early intervention and referrals are essential to prevent acute problems becoming chronic and to improve the chances of facilitating a return to work for absent employees.

6. Relevant policies and procedures

The employer has policies that may be relevant in managing individual cases where employee attendance is causing concern, and these should be applied alongside this policy where appropriate. They are:

- Disciplinary Procedure
- Grievance Procedure
- Company Vehicle policy
- Health and Safety Risk Assessment Policy

7 Attendance management

7.1 The employer will actively manage employee attendance to ensure appropriate and timely action is taken in individual cases where an employee's attendance falls below the standards expected.

7.2 Although the primary focus of this policy is attendance management rather than employee health, the employer will seek medical advice on individual cases wherever necessary to support employees in improving their attendance and to ensure the most appropriate policy or procedure is being followed.

7.3 The attendance management processes to be followed are set out below.

8 Return to work discussion

8.1 Where an employee returns to work following a period of absence the employer will have an informal discussion with them. The return-to-work discussion will take place following each period of absence regardless of the duration of the absence but will not be a mandatory requirement for absences authorised in advance by the employer e.g., jury service, special leave, etc.

8.2 A return to work discussion will normally take place within 48 hours of an employee's return to work but in any event should be completed within five working days of their return to work.

9 Trigger points for formal action

9.1 The trigger points for formal action under this policy are:

i. Five separate periods of absence in a rolling 12-month period, or
ii. Ten days consecutive or non-consecutive absence in a rolling 12-month period (pro rata for part-time employees).

9.2 In respect of 9.1(i), the number of separate occasions will not be pro rata for part-time employees.

10 Attendance management meetings

10.1 An employee will be required to attend a formal attendance management meeting (AMM) when the frequency and/or duration of their absences have reached a trigger point.

10.2 The AMM will usually take place within two weeks of the employee's return to work.

10.3 The employee will be given reasonable notice of an AMM, and they have the right to be accompanied by a work colleague if they wish. However, the AMM will not usually be delayed by more than five working days if the employee's chosen companion is not available.

10.4 The AMM will consider the employee's attendance record and all relevant factors and will

determine what action, if any, is required. Appropriate action can include the issuing of a formal warning alongside any other appropriate action to help the employee improve their attendance.

10.5 The outcome of the AMM, including any agreed actions, will be confirmed to the employee in writing, normally within five working days.

11 Issuing a warning for unsatisfactory attendance.

11.1 A formal warning will normally be issued unless there is a compelling reason why this would be inappropriate.

11.2 The purpose of the warning is to notify the employee that their absence is a cause for concern and that a failure to improve their attendance may lead to a further warning or it may lead to dismissal in cases where an employee triggers the policy while a stage 3 final written warning is live.

11.3 If the employee's absence is pregnancy-related a warning must not be issued.

11.4 If the employee's absence is because of a disability, the manager must seek further advice before any decision on whether to issue a warning is taken.

11.5 The levels of warning that can be issued under this policy are as follows:

11.6 Stage 1 – formal oral warning

A stage 1 warning will normally remain live for six months from the date of the AMM. If further absence occurs and the employee's absence remains at or above the trigger point while a stage 1 warning is live, the employee will be required to attend a further AMM, which may lead to a formal stage 2 warning.

11.7 Stage 2 – formal written warning

A stage 2 formal warning will normally remain live for 12 months from the date of the AMM. If further absence occurs and the employee's absence remains at or above the trigger point while a stage 2 warning is live, the employee will be required to attend a further AMM, which may lead to a formal stage 3 warning.

11.8 Stage 3 – final written warning

A stage 3 formal warning will normally remain live for 18 months from the date of the AMM. If the employee's attendance continues to be a cause for concern following the issue of a stage 3 formal warning i.e. the employee triggers the policy while a stage 3 formal warning is live, the manager may consider moving to a dismissal stage.

11.9 While the employer recognises that employees will have periods of genuine sickness absence for which they are not at fault, any warning given identifies that employees are not meeting the standards the employer requires for its employees. In deciding on the appropriate penalty under any procedure under which a warning may be given, the employer reserves the right to take account of any live warnings on the employee record made under that or any other procedure where appropriate to do so.

11.10 All warnings issued under this policy will be recorded on the employer's attendance management system and on the employee's personnel file.

12 Appealing against a warning

An employee may appeal against the issuing of a formal warning by writing to the employer within five working days of receipt of the written decision. The employer will arrange for the appeal to be heard by a different officer to that who made the initial decision to issue the warning.

13 Long-term sickness absence

13.1 The employer defines long-term absence as a period of continuous sickness absence of four weeks or more.

13.2 Once an employee has reached four weeks' continuous sickness absence, where appropriate, the employer will arrange to meet with the employee to discuss their health and any options which may help facilitate the employee's early return to work. The meeting can take place at the employee's home, at their normal place of work, or at another venue if, after consultation between the parties, this would be more appropriate. The meeting place should be reasonable, convenient for all and private so that the employee's confidentiality is not compromised. A meeting may not be needed if a return-to-work date is imminent.

13.3 Employees may be accompanied at this meeting by a work colleague, but this will not usually delay the meeting by more than five working days.

13.4 Formal contact at four weeks is the minimum level of contact required. The employer is expected to ensure that appropriate contact (by telephone, e-mail, or other appropriate means) takes place between them and the absent employee both before and after the four-week period.

13.5 The employer will need to consider whether the employee is disabled within the meaning of the Equality Act 2010 and consider any reasonable adjustments that may enable the employee to return to work.

13.6 If the employee is unlikely to return to work in the foreseeable future, the employer will need to consider whether dismissal is appropriate.

14 Consideration of dismissal

14.1 Dismissal will be considered under this policy in the following circumstances:

- Unacceptable levels of absence where the employee has an underlying health condition (ill-health incapability).
- Long-term sickness absence – no foreseeable return to work (ill-health incapability).
- Employee is at work but not performing full range of duties because of an underlying health condition (ill-health incapability).
- Unacceptable levels of absence where the employee has no underlying health condition (a dismissal in these circumstances may be for 'some other substantial reason').

14.2 If consideration of dismissal is appropriate, the employer will prepare a management report recommending dismissal for consideration by the Company Director. The report will include all relevant matters, including where applicable, up to date medical advice, details of any disability issues that need to be considered and any points made by the employee which were considered by the manager before deciding whether to recommend dismissal. For cases of ill-health incapability, consideration of ill health retirement will also need to be made at this stage.

14.3 The Director will consider the report and, if dismissal is being considered, the employee will be invited to attend a case review hearing at which they will have the right to be accompanied by a work colleague.

14.4 The employee will be provided with a copy of the management report under consideration at the meeting not less than three working days prior to the case review hearing.

14.5 The Company Director will consider all the relevant matters, and any further information provided by the employee at the case review hearing and will notify the employee of the outcome following the hearing. Where dismissal is considered appropriate, authority to dismiss and the timescales will be in accordance with the provisions of the company's disciplinary procedure.

14.6 If an employee is dismissed for unacceptable absence, they have the right of appeal. Refer to the Grievance and Disciplinary Procedures.

15.1 The employer will consider the requirements of the General Data Protection Regulations 2018 when requesting, recording, and monitoring information on individual sickness absence and will follow best practice guidelines as recommended by the Information Commissioner in the way it holds and shares information on absence records.

15.2 Any Company employee with responsibility for any stage of this policy and/or with access to confidential and sensitive data about employees' health are required to treat all information relating to individuals in accordance with the principles of the General Data Protection Regulations 2018. Failure to comply with those regulations data protection or any other standard may result in disciplinary action up to and including dismissal.

KEITH COOK TRAINING LTD DISCIPLINARY PROCEDURE

SCOPE

This procedure will be used only when necessary and as a last resort. Where possible, informal and/or formal counselling or other good management practice will be used to resolve matters prior to any disciplinary action being taken. The procedure is intended to be positive rather than punitive but takes heed of the fact that sanctions may have to be applied in some circumstances.

1. An employee can discuss any part of this policy with the Manager. They can help clarify an employee's rights as well as give guidance and support where it may be needed. Every individual has the right to representation by a work colleague at any point during the disciplinary process.

SUSPENSION

2. Suspension is not disciplinary action. Suspension can be used when it is necessary to remove a member of staff from the workplace pending an investigation for example, to allow time for a 'cooling down period' for both parties, for their own or others protection, to prevent them influencing or being influenced by others or to prevent possible interference with evidence. Only the Manager in charge of that individual has the authority to suspend an individual.

3. An employee suspended from duty will receive written confirmation within three days of:

- the reason for the suspension
- the date and time from which the suspension will operate.
- the timescale of the ongoing investigation.
- the right of appeal to the Company Director should the suspension last more than 7 days

COUNSELLING

4. Counselling is an attempt to correct a situation and prevent it from getting worse without having to use the disciplinary procedure. Where improvement is required, the employee will be given clear guidelines as to:
- what is expected in terms of improving shortcomings in conduct or performance
- the time scales for improvement
- when this will be reviewed
- the employee will also be told, where appropriate, that failure to improve may result in formal disciplinary action.

5. A record of the counselling will be given to the employee and a copy retained in their personnel file. Counselling will be followed up and improvements recognised and recorded. Once the counselling objectives have been met, any record of the counselling will be removed from the employee's file.

6. If during counselling it becomes clear that the matter is more serious, then the counselling process should be stopped and pursued under the formal disciplinary procedure.

PROCEDURE FOR FORMAL INVESTIGATION

7. Formal investigations will be carried out by the most appropriate officer who is not directly involved with the incident being investigated. This officer may involve others to assist with the investigation process. All the relevant facts should be gathered promptly as soon as is practicable after the incident. Statements should be taken from witnesses at the earliest opportunity. Any physical evidence should be preserved and/or photographed if reasonable to do so.

8. A report should be prepared which outlines the facts of the case. This should be submitted to the Managing Director who will decide whether further action is required. Where appropriate, this report may be made available to the individual and their representative.

9. In most circumstances where misconduct or serious misconduct is suspected, it will be appropriate to set up an investigatory hearing. This will be chaired by the Managing Director who will be accompanied by another manager if possible. The investigating manager would be asked to present their findings. Witnesses should be called at this stage, and the employee (or their representative) allowed to question these witnesses. The employee has a right of representation at this hearing.

10. Following the full presentation of the facts, and the opportunity afforded to the employee to state their side of the case, the hearing should be adjourned, and everyone would leave the room except the Managing Director hearing the case, and the other manager. They would discuss the case and decide which of the following options was appropriate:

- take no further action against the employee
- recommend counselling for the employee
- proceed to a disciplinary hearing

11. All parties should be brought back and informed as to which option has been chosen. Should the decision be taken to proceed to a disciplinary hearing, then this may follow on immediately from the investigatory hearing if the following criteria have been met:

- the employee has been informed by letter that the investigation may turn into a disciplinary hearing, and that they have the right of representation
- they have been told in advance what the nature of the complaint is, and had time to consult with a representative
- all the facts have been produced at the investigatory hearing, and the Managing Director is in a position to decide on disciplinary action.

12. The manager should inform the employee and their representative that the hearing would now become a formal disciplinary hearing and invite them to say anything further in relation to the case.

13. It may be appropriate at this point, at the discretion of the manager hearing the case, to adjourn proceedings. This might be for several reasons e.g., whilst necessary arrangements are made for a representative to attend the hearing at the request of the employee, or if the employee has become emotional or distressed.

14. Should anyone who is subject to disciplinary action resign during the course of it, the action will cease unless there are extenuating circumstances which require it's continuance. The subject of the discipline may also request that the disciplinary action continue.

WARNINGS

Examples of Minor Misconduct

15. Below are listed examples of misconduct which may warrant either a Verbal Warning or a First Written Warning. It is stressed however that this list is not exhaustive and that on all occasions a full and proper investigation will take place prior to the issue of a warning.

- Persistent lateness and poor timekeeping.
- Absence from work, including going absent during work, without valid reason, notification, or authorisation.
- Failure to work in accordance with prescribed procedures.
- Unreasonable standards of dress or personal hygiene.
- Failure to observe company regulations and procedures.

Verbal Warning

16. A Verbal Warning is appropriate when it is necessary for the manager in charge to take action against an employee for any minor failing or minor misconduct.

First Written Warning

17. A First Written Warning is appropriate when:
- a verbal warning has not been heeded and the misconduct is either repeated or performance has not improved as previously agreed.
- an offence is of a more serious nature for which a written warning is more appropriate.
- the recurrence or accumulation of an offence/offences, if left, will lead to more severe disciplinary action.

Examples of Gross – Misconduct

18. Listed below are examples of misconduct which may be considered to be Gross Misconduct and may warrant a Final Warning or Dismissal. This list is not exhaustive, and, on all occasions, a full and proper investigation will take place prior to the issuing of a Final Warning or Dismissal.
- Theft, including unauthorised possession and/or use of Company property.
- Breaches of confidentiality, prejudicial to the interest of the business,
- Being unfit for duty because of the misuse/consumption of drugs or alcohol.
- Refusal to carry out a management instruction which is within the individual's capabilities, and which would be seen to be in the interests of the business.
- Breach of confidentiality / security procedures.
- Physical assault, breach of the peace or verbal abuse.
- False declaration of qualifications or professional registration.
- Failure to observe business rules, regulations, or procedures.
- Wilful damage of property at work.
- Incompetence or failure to apply sound professional judgement.
- Bribing or attempting to bribe another individual, or personally taking or knowingly allowing another person to take a bribe.

Final Written Warning

19. A Final Written Warning is appropriate when:
- an employee's offence is of a serious nature falling just short of one justifying dismissal.
- an employee persists in the misconduct which previously warranted a lesser warning.

Dismissal

20. Dismissal is appropriate when
- an employee's behaviour is considered to be Gross Misconduct.
- an employee's misconduct has persisted, exhausting all other lines of the disciplinary procedure.

Time Scales for the expiry of Warnings

21. Warnings issued to employees shall be deemed to have expired after the following periods of time.

- Verbal Warnings: 6 months
- First Written Warnings: 12 months
- Final Written Warnings: 18 months (or as agreed and recorded at the hearing)

22. These time scales remain provided that during that period, no further warnings have been issued in respect of the employee's conduct.

LETTER OF WARNING

23. All warnings will contain the following information:
- The letter will be issued within 7 days of the date of the disciplinary hearing.
- The nature of the offence and where appropriate, that if further misconduct occurs, more severe disciplinary action will be taken.
- The period of time given to the employee for improvement.
- The employees right to appeal to the manager directly above that of the one issuing the warning.
- A copy of the warning and any supporting documentation will be attached to the individual's personnel file.
- The employee will also receive a copy of the warning which in the case of any written warning will be sent to their home address by recorded delivery if not handed to them in person.
- In the case of a final written warning, reference will be made to the fact that any further misconduct will lead to dismissal, and that the employee has the right of appeal, and to who they can make that appeal.

24. The letter confirming dismissal will contain the following information:
- The reason for dismissal and any administrative matter arising from the termination of their employment.
- The employees right of appeal and to whom they should make that appeal

APPEALS

25. Every employee has the right to appeal against the outcome of a disciplinary hearing. The basis of an appeal should normally relate to one of the following areas:
- that the Company's' procedure had not been followed correctly.
- that the resulting disciplinary action was inappropriate.
- that the need for disciplinary action was not warranted.
- that new information regarding disciplinary action has arisen

26. An appeal should be put in writing to the manager who issued the disciplinary warning / dismissal. The letter of appeal may be constructed by the employee or their representative. The letter should contain the grounds for appeal and should be lodged within 10 days of receipt of the warning / dismissal letter.

27. An appeal will be arranged within 20 working days of receipt of the appeal letter.

Appeals against Verbal and First Warnings

28. In the case of verbal and first warnings, the appeal will be heard by the manager next in line to the one who issued the warning.

29.

Appeals against Final Warnings and Dismissal

30. The hearing and determining of appeals against final warnings and dismissal will be heard by the Managing Director. If possible, they may also involve another officer not previously involved with the case.

31. When dealing with an appeal against a Final Warning or Dismissal the appellant may submit a written statement for consideration by the person(s) hearing the appeal

32. The person(s) hearing the appeal may consider the appeal based on the information previously available including the investigation report, and any submissions made by the appellant. They may at their discretion seek any further information which they feel would help them to come to a fair conclusion. The decision of the person(s) hearing the appeal are final and no further right of appeal is available.

KEITH COOK TRAINING LTD GRIEVANCE PROCEDURE

This grievance procedure is intended as the tool by which a member of staff may formally have a grievance, regarding any condition of their employment, heard by the management of the Company. The aggrieved employee has the right to representation by a work colleague.

In the event of a member of staff wishing to raise a grievance, it is preferable for the grievance to be satisfactorily resolved as close to the individual and their line manager as possible. It is understood however that this is not always possible and that a formal procedure is required to ensure the swift and fair resolution of matters which aggrieve employees.

Time scales have been fixed to ensure that grievances are dealt with quickly, however these may be extended by agreement.

This procedure is not intended to deal with:

- Dismissal or disciplinary matters which are dealt with in a separate procedure.
- Disputes, which are of a collective nature.

Stages of the Procedure

Stage 1

An employee who has a grievance, should raise the matter with their manager / supervisor immediately either verbally or in writing. If the matter itself concerns the employee's immediate manager, then the grievance should be taken to their superior.

If the manager is unable to resolve the matter at that time, then a formal written grievance form should be submitted (see appendix 1). The manager should then respond within 2 working days (i.e., the managers normal working days) to the grievance unless an extended period is agreed upon by both parties. The response will give a full written explanation of the manager's decision and who to appeal to if still aggrieved.

Stage 2

In most instances, the Company would expect the manager's decision to be final and for the matter to end. However, in some circumstances the employee may remain aggrieved and can appeal against the decision of the manager concerned.

The appeal, to the manager next in line, must be made within ten working days of the original response to the employee's grievance. The appeal must be in writing (see appendix 2) and contain the original formal grievance form. This manager will attempt to resolve the grievance. A formal response and full explanation will be given in writing, as will the name of the person to whom they can appeal if still aggrieved, within 7 days.

Where the 'next in line' manager at this stage is the Director with responsibility for the employee's function, then the grievance should immediately progress to stage 3.

Stage 3

If the employee remains aggrieved there will be a final level of appeal to the Director responsible for the employee's function. This appeal must be made in writing (see appendix 3), enclosing a copy of the original formal grievance form, to the Director within ten working days of receipt of the Stage 2 response. The Director will arrange and hear the appeal with, where possible, another management representative and respond formally with a full explanation within 20 working days.

Where a grievance is raised against a director then the grievance will be heard by the Chief Executive.

There is no further right of appeal. Where however both parties agree that there would be some merit in referring the matter to a third party for advice, conciliation or arbitration, arrangements will then be made to find a mutually acceptable third party.

Using mediation

An independent third party or mediator can sometimes help resolve grievance issues before it is necessary to invoke the formal procedure. Mediation is a voluntary process where the mediator helps two or more people in dispute to attempt to reach an agreement. Any agreement comes from those in dispute, not from the mediator. The mediator is not there to judge, to say one person is right and the other wrong, or to tell those involved in the mediation what they should do. The mediator oversees the process of seeking to resolve the problem but not the outcome.

There are no hard-and-fast rules for when mediation is appropriate, but it can be used:

- for conflict involving colleagues or between a line manager and their staff
- at any stage in the conflict as long as any ongoing formal procedures are put in abeyance
- to rebuild relationships after a formal dispute has been resolved
- to address a range of issues, including relationship breakdown, personality clashes, communication problems and bullying and harassment.

Mediation is not part of the formal grievance procedure. However, if both parties agree to mediation, then the grievance procedure can be suspended to resolve the grievance through that route. If mediation is not successful, then the grievance procedure can be re-commenced.

KEITH COOK TRAINING LTD (the 'Company') TRAINING AND DEVELOPMENT POLICY

1 Introduction

1.1 This document forms the Company's Training and Development Policy. It sets out:

- The Company's commitment to training
- The identification of training needs
- Corporate training
- Financial assistance
- Study leave
- Short courses/workshops
- Evaluation of training
- Links with other policies
- Reporting on progress

1.2 The objectives of this document are to:

- Encourage employees to undertake appropriate training
- Allocate training in a fair manner
- Ensure that all training is evaluated to assess its value

2 Commitment to Training

2.1 The Company is committed to the ongoing training and development of all employees to enable them to make the most effective contribution to the Company's aims and objectives in providing the highest quality representation and services for customers.

2.2 The Company recognises that its most important resource is its staff and is committed to encouraging them to enhance their knowledge and qualifications through further training. Some training is necessary to ensure compliance with accrediting bodies and/or all legal and statutory requirements.

2.3 The Company expects staff to undertake a programme of continuing professional development (CPD) in line with the requirements of their requisite professional bodies.

3 The Identification of Training Needs

3.1 Staff will be asked to identify their training and development needs with advice from the manager during their annual appraisal or regular meetings. There are number of additional ways that the training needs of staff may be recognised:

- During interview
- Following confirmation of appointment.
- Formal and informal discussion

3.2 Other circumstances may present the need for training:

- Legislative requirements i.e. First Aid, Fire Safety, Manual Handling.
- Changes in legislation and/or accrediting body requirements
- Changes in systems
- New or revised qualifications become available
- Accidents
- Professional error
- Introduction of new equipment
- New working methods and practices
- Complaints to the Company
- A request from a member of staff
- Delivery of new services

3.3 Staff who wish to be considered for a training course should discuss this in the first instance during their appraisal; where it will be determined whether the training is relevant to the Company's needs and/or service delivery.

4 Corporate Training

4.1 Corporate training is necessary to ensure that staff are aware of their legal responsibilities or corporate standards e.g., Health and Safety, Risk Management and Equal Opportunities. Staff will be required to attend training courses, workshops, or seminars where suitable training is identified.

5 Financial Assistance

5.1 It is important to note that all training must be appropriate to the needs of the Company, be relevant to the individual's role and is subject to the availability of financial resources.

5.2 Each request will be considered on an individual basis and the benefits to the individual and the Company will be identified.

5.2 For approved courses staff can expect the following to be sponsored.

- The course fees
- Examination fees
- Associated membership fees
- One payment to re-take a failed examination
- Subsistence

5.3 Failure to complete any course of training may result in the Company withdrawing future training and requesting the refund of financial assistance. Each case will be considered on an individual basis.

5.4 Any employee undertaking training funded by the Company must be aware that should they leave KCTL employment within two years of completion of the qualification they will be required to repay all costs associated with the undertaking of such training.

5.5 Where attendance is required at courses a full day of paid leave will be granted for each completed day of the course.

6 Evaluation of Training

6.1 Records of all training undertaken by staff will be kept in the personnel files of each member of staff.

6.2 As part of the Company's commitment to training and development, staff are asked to provide feedback on the value and effectiveness of the training they undertake highlighting in particular the key implications of new legislation, guidance and/or best practice for the ongoing efficiency and effectiveness of the Company.

7 Linking with other Company Policies and Statutory Requirements

- Equality of opportunity in all aspects of staff development
- Health and Safety Policy – ongoing training and development is key to ensuring a positive approach to Health and Safety is embedded throughout the Company
- Undertaking training is a clear indication of Continuing Professional Development.

8 Conclusion

The adoption of this training policy will achieve many benefits for the Company. It will assist in demonstrating that the Company is committed to continuing professional development and enhancing the skills of staff.

9 Freedom of Information

In accordance with the Freedom of Information Act 2000 this Document will be available for inspection in the employee handbook.

Working Time Agreement

Working hours are full-time: 40 per week or averaging 40 per week.

The Company's core hours, between which you are required to be at work as a minimum, are 8.30am to 4.30pm. During these core hours you will be expected to be available or at work (whether present at the head office or working remotely) during a core period on each of your working days. Outside of this, your start and finishing times may vary according to your individual or customer preference and business need and will not exceed an average of 40 hours in total each week.

You will have a lunch break of 30 minutes per day which is not working time, and which is not paid.

The employer and/or the accrediting body will be responsible for determining the training hours and standards that are required on each course.

If the employee at any time does have a preferred working time the employer will do its best to accommodate this. However, the employer reserves the right to refuse a request in circumstances where the operation of the business would be adversely affected. Any requested changes to working hours is deemed to be a discretionary benefit and not a contractual right and may be withdrawn at any time.

For the purposes of this agreement the full-time working hours include any travel time to and from training venues. However, the employer recognises that it does have a duty of care in accordance with the Health and Safety at Work etc Act 1974 to take appropriate steps to ensure the health and safety of its employees and others who may be affected by their activities when at work. This includes the time when they are driving in a company vehicle.

There will always be risks associated with driving. Although these cannot be completely controlled, the employer has a responsibility to take all reasonable steps to manage these risks and do everything reasonably practicable to protect people from harm in the same way as they would in the workplace.

Accordingly, the following arrangements will apply:

- If the training location is less than 75 miles from the head office the employee will be expected to make the return journey on the same day.

- If the training location is between 76 and 100 miles from the head office and the course is more than two days in duration the employee will be offered the option of using overnight accommodation at a time to take into account the customer preference or business need. If the employee declines this arrangement, then they will be expected to make the return journey on the same day in which case they will have chosen to work longer and 'opt out' of the provisions of the Working Time Regulations 1998.

- If the training location is more than 101 miles from the head office and the course is more than two days in duration the employee will use overnight accommodation as determined by the employer. If the employee declines this arrangement and choses to make the return journey on the same day, they will have chosen to work longer and 'opt out' of the provisions of the Working Time Regulations 1998.

This policy applies to all employees apart from freelance instructors, additional workers, and third-party agency workers. They will be individually contracted to work hours as appropriate to the nature of the work that they are doing or any specific operational requirements.

Key points

The operation of this agreement is based on trust and responsibility. In return the employer expects the employee to be responsible about completing their contractual hours.

If the employee is suspected of abusing this agreement action may be taken in accordance with the employer's disciplinary procedure.

If the employee feels that any decision concerning individual requirements hasn't been fair, then the employer's grievance procedure should be followed.

Policy Statement: CCTV

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act in respect of the use of CCTV (closed circuit television) surveillance systems managed by Keith Cook Training Limited and is registered with the ICO.

The CCTV System includes static and remotely operated cameras and is used for the purpose of:

The prevention, detection, and investigation of criminal activity.

The security of the premises.

Surveillance & Audio in ITC Rooms; and

Safeguarding the safety of students, staff, and visitors.

The CCTV system is registered with the Information Commissioner.

Responsible Person

The person who has been appointed to oversee the system and procedures is:

Managing Director

Images recorded.

Signs are displayed to notify all users that CCTV is in operation.

The images that are filmed are held in a secure location and can only be accessed by those who are authorised to do so.

Digital media is used to record images and audio for quality assurance processing.

The system has been set up to provide good quality images.

Every camera records simultaneously and the images are stored on disc for a period of 30 days. After that time all images are erased apart from any which relate to an incident subject to an ongoing investigation, these can be recorded to compact disk.

Routine checks are made to ensure that the system is operating in accordance with the terms of this policy, and that information relating to the recordings (date, time etc) are accurate.

All Policies and procedures outlined within this document including any section have been read and understood by the individuals below and have accepted this document in its entirety.

Part 5 - Safety Rules for Contractors, Registered Instructors, Assessors, and Internal Verifiers.

It is a condition of all registered instructors, assessors, internal verifiers, contractors, or agents who may work for Keith Cook Training Limited to abide by all health and safety rules, policies, and procedures, including the following safety rules, currently in effect at Keith Cook Training Limited.

Keith Cook Training Limited is committed to high safety standards, and they regard Health and Safety at Work as being of paramount importance. It must be clearly understood by every registered instructor, assessor, internal verifier, contractor, and agent, before the commence work on behalf of Keith Cook Training Limited that they will be aware of all health and safety regulations and ensure compliance with their obligations both at Common and Statute Law.

Responsibilities

It is the responsibility of the registered instructor, assessor, internal verifier, contractor, or agent to make themselves familiar with, and compliant with, any obligations and statutory duties applicable to their work. Approved Codes of Practice and Guidance notes must be used as reference where appropriate. Any additional requests in the interests of health and safety must be complied with.

Contractors, Registered Instructors, Assessors, and Internal Verifiers are responsible for: **-**

- The safety and security of any plant and materials that may be brought onto Keith Cook Training Limited or clients' premises.

- Obtaining permission to sue Keith Cook Training Limited equipment (such equipment must be used in a safe and proper manner). All registered instructors, contractors or agents using Keith Cook Training Limited equipment accept responsibility for such equipment and accept liability for any subsequent loss or damage.

- Any of Keith Cook Training Limited tools or equipment requiring servicing or maintenance are brought to the attention of Keith Cook Training Limited management.

- Ensuring that tools and equipment are used only by adequately trained persons, unless undergoing training under supervision.

- The safety of trainees at all times.

Alcohol and Drugs

Instructors, assessors, internal verifiers, sub-contractors, or agents will not bring onto Keith Cook Training Limited premises, or the premises or sites of any of their clients, sell, give, barter or otherwise dispose of any alcoholic liquor, drugs or any other such product. The exception will be prescribed drugs for personal use, where such use will not impair the ability of the individual to operate plant or machinery.

Instructors, assessors, internal verifiers, contractors, or agents shall not permit the consumption or presence of any alcoholic liquor or drugs (except prescribed drugs for personal use) on any premises or sites at any time. Nor shall the instructor, assessor, internal verifier, contractor or agent or anyone employed or being trained by them be allowed to be present on the premises or site if such a person is judged to be under the influence of any intoxicating liquor or drug.

Any person contravening this requirement will be removed from the premises or site by any person appointed by Keith Cook Training Limited or their client.

Smoking

Smoking is not permitted in any classroom, office or enclosed rest rooms on Keith Cook Training Limited premises, or client's site, by trainees, registered Instructors, assessors, internal verifiers, sub-contractors, or agents.

No-one will be permitted to operate any plant or machinery whilst smoking.

Smoking in any company owned vehicle is expressly forbidden.

Accident Reporting Procedure

- All accidents and incidents, however minor, must be reported to the Head Office of Keith Cook Training Limited, by the instructor on the day on which the accident or incident occurred.
- In the event of an accident involving personal injury, or significant damage to property or equipment, the report should be made immediately by telephone, text message or fax.
- The instructor must complete an Accident Report Form and ensure that this reaches Head Office without delay, if possible, to arrive on the day of the accident, but in any case, within three working days.
- If any treatment was given at the scene, details must be provided on the accident report form.
- If the accident is reportable under RIDDOR Keith Cook Training Limited will immediately notify the employer who will report the accident to the HSE.
- The instructor, if possible, should take photographs of the accident, showing details of the location, equipment, damage caused.
- In the case of a reportable accident, the instructor must ensure that s/he has full contact details of all course participants and any other witnesses who may later be required to provide evidence.
- Witnesses should be asked to provide a written account of the accident or incident to Head Office as soon as possible.
- Head Office will forward documentation as appropriate to insurance companies and/or accrediting bodies. In the case of Training Courses run under specific accreditation, the reporting and investigation procedures of the appropriate accrediting body will take precedence.

Accident Investigations

If the accident is reportable and HSE decide to investigate, they will contact KCT Ltd for confirmation that the course was run by a registered instructor who was approved for that course.

- The relevant Technical Adviser will review the Accident Report Form, accompanying documentation and photographs. They will also contact the instructor concerned to offer support and to seek clarification or further information where necessary.
- Depending on the outcome of the Technical Advisor's review, the follow actions may be taken by KCT Ltd.
    - Internal Monitoring System (IMS) Quality Audit.
    - Information which may help to avoid similar accidents occurring in the future being disseminated to KCT Ltd instructors through appropriate channels.
    - Changes to risk assessment procedures.
    - Logging as an opportunity to improve.

NVQ/QCF/Adult Apprenticeships - Accidents to employed candidates on employer's site, outside of assessment periods.

- Candidates registered on any form of training and/or assessment program offered by Keith Cook Training Limited are fully employed and therefore the responsibility for ensuring adherence to health and safety rules at the employer's site or sites lies with the employer.
- Any reporting under RIDDOR is the responsibility of the employer.
- The employer will carry out a full accident investigation, with appropriate amendments to safe systems of work, method statements etc as required by their internal health and safety procedures.
- As soon as the assessor or instructor is notified of an accident involving a registered candidate, the centre manager must be informed.
- When the candidate is funded through a government scheme, the centre manager will notify the relevant people within the funding agency and amend the candidate's status accordingly.
- Full details of the accident report and revised control measures will be requested from the employer and forwarded to the funding agency.

Company Vehicle Policy – Also See Company Vehicle Incident Procedures on Page 165

Keith Cook Training Ltd (the 'Company')

Vehicle Policy

Policy overview.

This vehicle policy gives employees guidelines for using a company vehicle. A "company vehicle" is any vehicle allocated to an employee. This policy applies to all employees who use a company vehicle and applies during and outside of working hours.

Qualifying for a company vehicle.

Employees qualify for a company vehicle if they need a company vehicle for their daily work.

To be eligible for a company vehicle, employees must submit a copy of their driver's licence. Employees are only allowed to drive a company vehicle if they have a valid driver's licence and a clean driving record for at least [X years].

A clean driving record means the employee has not been held at fault for a car accident or arrested on charges of contravening vehicle and traffic legislation. The company can give or remove access to a vehicle at its discretion.

Company vehicles for employees with disabilities.

The company will make reasonable adjustments to facilitate company vehicle use for eligible employees with disabilities.

Company vehicle rules.

Obey traffic legislation and be courteous toward other drivers.

Complete driving records as instructed.

Monitor fuel and refill the vehicle as required using the fuel card provided by the company. The fuel card cannot be used for refuelling any vehicle other than that allocated to the employee.

Monitor tyre pressure, lights, and all fluid levels.

Report any damage or problems to your vehicle immediately.

Report changes to your driver license categories, such as penalty points, licence suspension, immediately.

Always lock company vehicle.

Any tools, equipment or items of value must be removed from the vehicle overnight.

Bring vehicle to scheduled maintenance appointments.

Do not drive while under the influence of alcohol, fatigued, or on medication that affects your driving ability.

Do not smoke in any company vehicle.

Do not lease, sell, or lend a company vehicle.

Do not use a phone or text while driving.

Keep the vehicle in a clean condition both internally and externally. Where permitted the company fuel card can be used for the exterior valeting of vehicles.

Do not allow unauthorised drivers to use a company vehicle unless required by an emergency.

Employees who contravene vehicle rules will subject to action in accordance with the company's disciplinary policy which may include verbal and written warnings, withdrawal of vehicle use, replacement of tools, equipment, or items of value at their own expense, termination of employment or legal action.

Accidents.

Contact the administration office immediately. They will contact the company's insurance provider.

Follow legal guidelines for exchanging information with other drivers and report the accident to local police if required.

Do not guarantee payment or accept responsibility without company authorisation.

The Company's responsibilities.

Ensuring vehicles are safe before allocating them to the employee.

Scheduling regular maintenance.

Providing car insurance.

Retiring and replacing cars as needed.

What the Company is not responsible for.

Motoring offences and/or paying parking or traffic fines employees receive while driving company vehicles they are responsible for.

Paying any other costs that arise as a result of those motoring offences and/or fines such as time off for court appearances and any penalties that may be imposed.

Paying any legal costs for employees who are arrested while driving company cars.

Equal Opportunities Policy

Keith Cook Training Limited is aware of its responsibilities under the Health and Safety at Work Act and the Approved Codes of Practice relevant to the industry. The Equality Act 2010 legislation must take priority over Equality of Opportunity and where the inclusion of persons who do not meet the specifications laid down in the ACOP would breach Health and Safety regulations, such individuals will not be accepted on training, testing or assessment programs.

Employment

Keith Cook Training Limited will make no discrimination in its recruiting campaigns and employment of permanent or temporary staff, on the grounds of physical or sensory disability, race, colour, creed, sex or age of applicants. All positions will be filled on the basis of appropriate skills and experience.

Records of all recruiting campaigns will be maintained and decisions to employ will be made on the grounds of the best qualified person for the job.

Keith Cook Training Limited will not pursue any recruiting campaign which seeks to favour any specific group on the basis of ethnicity, sex or age.

Access to Training, Testing and/or Assessment

Keith Cook Training Limited recognises the need for access to NVQ assessment to be open to all, regardless of physical or sensory disability, race, colour, creed, sex, or age. Wherever possible with due regard to Health and Safety requirements, Keith Cook Training Limited will: -

- Provide a flexible registration and pricing policy to enable access for those with single unit specific training requirements as well as for those within extended programmes of training.
- Provide on demand assessment for internal or external candidates for single unit or full qualification certification.
- accept all valid assessment methods and adaptations of standard approaches to assessment to enable assessment for those with special assessment needs.
- Accept all valid prior evidence of achievement in assessing evidence of competence.
- Assess evidence only against an individual's demonstration of competence to the specified standards.
- Regularly send representatives to brief and training events organised by the Awarding or Accrediting Body.

Access to Training

Keith Cook Training Limited will ensure that access to all forms of training is provided irrespective of physical or sensory disability, race, colour, creed, sex, or age. Wherever possible with due regard to Health and Safety requirements, Keith Cook Training Limited will:

- Ensure any computer equipment, used by trainees can be configured to activate accessibility options and that appropriate members of staff can activate all accessibility options.
- Ensure that trainers understand how to communicate through an interpreter, and actively encourage learners whose first language is not English to bring an interpreter with them for both training and testing sessions.
- Ensure that all trainers are aware of the needs of other creeds, particularly in terms of timing for breaks, food offered and arrangements for privacy.
- Ensure that no trainer uses or permits any form of discriminatory language or behaviour within the training centre.
- Allow trainees to use appropriately modified equipment to overcome physical disabilities, where this does not affect a trainee’s safety.

Preventing Discrimination

Instructors working with Keith Cook Training Limited will treat equally and fairly all delegates irrespective of their colour, race, creed, sex, age, or any learning, physical or sensory disability, where this does not affect their ability to operate plant safely and/or perform manual tasks associated with the operation of the plant on which they are being trained and/or assessed.

Instructors, trainers or assessors who witness any discriminatory behaviour in the learners under their supervision will ask the learner to leave the training room and will report the incident immediately to George Walton who will investigate the incident and refer to Keith Cook for a final decision on action to be taken.

Course notes and training aids will be so designed as to treat equally and fairly all delegates irrespective of their colour, race, creed, sex, age, or any learning, physical or sensory disability.

Monitoring

Keith Cook Training Limited will develop and maintain a system for monitoring the effectiveness of its equal opportunity policy and procedure, in accordance with the requirements of the appropriate awarding body.

Training courses will be monitored, at intervals, against the requirements of the current QCF unit applicable to classroom delivery. Records will be held in the centre. Before accepting contracts from employers for training and/or assessment, Keith Cook Training Limited will check that employers promote a similar equal opportunities policy.

Procedures will be regularly reviewed to ensure that delegates are selected and trained on their merits and abilities and that direct or indirect discrimination does not occur.

Prevention of Discrimination Policy

For the purposes of this policy, bullying is defined as any inappropriate behaviour or use of language which may intentionally or unintentionally cause offense to others or have the effect of excluding or discriminating against individuals.

As an equal opportunity's employer, Keith Cook Training Limited supports a working environment for individuals in which safety is of paramount importance. The purpose of this policy is to support a working environment and culture in which all staff, trainees, visitors are treated with respect.

All members of staff at Keith Cook Training Limited will be made aware of the negative effects of inappropriate and discriminatory behaviour, both direct and indirect, and will actively work to ensure that any instances of such behaviour are correctly reported.

Any incidents of bullying, harassment, or any other form of unacceptable behaviour by a learner or a member of staff should be reported to George Walton. A thorough investigation will be carried out.

All such complaints and investigations will be treated in confidence.

Keith Cook Training Limited reserve the right to exclude anyone who is proven to deliberately cause offence to others from further training and/or assessment.

All members of staff will be encouraged to undertake periodic training to ensure their knowledge of current employment law relating to unacceptable, discriminatory behaviour in the workplace is up to date.

Children and Vulnerable Adults Policy

Under Health and Safety regulations as related to Construction sites, children, and vulnerable adults with severe learning difficulties or physical or sensory disabilities are prohibited on the premises. This restriction applies equally to all training related to the operation and use of construction plant and industrial forklift trucks.

People with minor learning difficulties, egg dyslexia, are supported on an individual basis throughout their training and assessment periods, as dictated by individual needs.

Interpreters can be made available where necessary to speakers of languages other than English, and the deaf. Those in need of an interpreter are free to bring an interpreter of their own choice to any training or assessment meeting, with prior notification to the centre management.

No-one under the age of eighteen is permitted to operate a forklift truck within a warehouse, and therefore this restriction applies equally to the training of young people on our premises.

School leavers may be employed in a warehouse in a role other than operating forklift trucks, and these individuals may attend training sessions, for example in manual handling, relevant to their work.

Children over thirteen are permitted to learn to drive an agricultural tractor for use on fields only. One course per year operates for a maximum period of three days in the summer months.

When young people under the age of eighteen attend training at our premises only instructors who have a clear CRB check will be used, and the welfare officer will be introduced during induction.

Also see safeguard Policy & Procedures within this document.

Lone Worker Policy

Keith Cook Training Limited recognises that there may be times when its employees work alone and that it has responsibilities for their health, safety, and welfare. Keith Cook Training Limited takes these responsibilities seriously and has developed control measures and training to reduce risk.

Prior to entering any situation where an employee is likely to be working alone, the following extra risk control measures are taken, informally or formally as appropriate to the situation.

1) An assessment of whether the location presents a special risk:
    a) Assessing the likelihood of violence or aggression.
    b) Assessing any special risk if the employee is a woman.
    c) Assessing any special risk if the employee is young.
2) Ensuring that employees have no medical condition that makes them unsuitable for working alone, including pregnancy.
3) Training is carried out in emergency procedures and to control situations of uncertainty.
4) Only experienced, fully qualified, and competent employees are permitted to work alone.
5) Ensuring that the employee informs Keith Cook Training Limited of their location and expected length of meeting or event, and estimated time of return to the office.
6) A mobile telephone is to be carried at all times during lone working.
    a) To advise the office of any problems experienced in travelling to a lone working location
    b) To advise the office of safe arrival at the lone working location
    c) To advise the office or seek advice from the office in case of any unanticipated situations.
    d) To advise the office of departure from the lone working location
    e) To advise the office of safe arrival at home if return is outside office hours.
    f) Mobile phones may not be operated whilst driving any vehicle, whether hands free or not.
7) Checks are made to ensure that the employee has returned after lone working.
8) A supervisor may occasionally visit and observe people working alone, alternatively the supervisor may contact the lone worker via mobile phone during extended periods of lone working.
9) Prior to an employee entering a lone working situation, decisions are made as to the limits of what can and what cannot be done when working alone, also ensuring that the employee is competent to handle new situations that may be beyond the scope of training.
10) This policy is reviewed and updated regularly to take into account experience gained and suggestions and amendments from its users.

Data Protection Policy General Data Protection Regulation (GDPR)2018

(Formerly Data Protection Act 1998)

PRIVACY NOTICE

BACKGROUND:

Keith Cook Training Ltd (KCTL) understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of all our customers and will only collect and use personal data in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

1. Information About Us

Keith Cook Training Ltd
Limited Company registered in England under company number: 7059714
Registered address: Springfield Farm, Charley Road, Oaks in Charnwood, Leicestershire, LE12 9YA.
VAT number: 9829055777
ICO Registration No: Z2368687
Data Protection Officer: George Walton
Email address: admin@kcts.me.uk
Telephone number: 01509 600330
Postal Address: Springfield Farm, Charley Road, Oaks in Charnwood, Leicestershire, LE12 9YA
We are regulated by all the awarding & accredited bodies we deliver under for training & qualifications.

2. What Does This Notice Cover?

This Privacy Information explains how we use your personal data: how it is collected, how it is held and how it is processed. It also explains your rights under the law relating to your personal data.

3. What is Personal Data?

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'. Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.
The personal data that we use is set out in Part 5, below.

4. What Are My Rights?

Under the GDPR, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 11.
b) The right to access the personal data we hold about you. Part 10 will tell you how to do this.
c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 11 to find out more.
d) The right to be forgotten, i.e., the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 11 to find out more.
e) The right to restrict (i.e., prevent) the processing of your personal data.
f) The right to object to us using your personal data for a particular purpose or purposes.
g) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 11.
Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

5. What Personal Data Do You Collect?

We may collect some or all the following personal data (this may vary according to your relationship with us).
• Name
• Date of birth
• National Insurance Number
• Gender
• Address
• Email address
• Telephone number
• Business name
• Job title
• Profession
• Payment information.
• Information about your preferences and interests
• Previous qualifications
• Information on disabilities, learning difficulties, ethnicity is required on funded learning as part of the Individual Learner Record as required by the Enterprise & Skills Funding Agency (ESFA).

6. How Do You Use My Personal Data?

Under the GDPR, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it.

• As a training provider we are classed as a processor of your information and will therefore process personal data supplied to us to fulfil the contract of delivering training and processing certificates.
• We only share data with organisations that support the training and certification of our learners, none of which are outside the EU
• We deliver training courses to learners on behalf of their employers. To understand the requirements of the learners we record and store the data in Part 5.

Your personal data will be used for or may be used for one of the following purposes:

• Registration of your qualification or exam with the awarding bodies
• Certification of your qualification or exam with the awarding bodies
• Supplying our services to you. Your personal details are required in order for us to enter into a contract with you.
• Personalising and tailoring our services for you.
• Communicating with you. This may include responding to emails or calls from you.
• Supplying you with information by email and post that you have opted-in to (you may unsubscribe or opt-out at any time by emailing us at admin@kcts.me.uk; SUBJECT: OPT OUT)

With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email, telephone, text message and post with information, news, and offers on our services. You will not be sent any unlawful marketing or spam. We will always work to fully protect your rights and comply with our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003, and you will always have the opportunity to opt-out.

7. How Long Will You Keep My Personal Data?

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the following periods (or, where there is no fixed period, the following factors will be used to determine how long it is kept):

• Personal data for the qualifications achieved by our learners is stored for lifetime via the registered awarding bodies and learner records services. You will have the right to access your learning records at any time.

• We keep and manager learning records for our customers in our own secure storage systems, all of which are GDPR compliant. This ensures secure access to information of personal learning records when required.

• We only store data with organisations that support the training and certification of our learners, none of which are outside the EU.

8. How and Where Do You Store or Transfer My Personal Data?

We will only store or transfer your personal data in the UK. This means that it will be fully protected under the GDPR.

9. Do You Share My Personal Data?

We only share data with organisations that support the training and certification of our learners.
We will not share any of your personal data with any other third parties for any purposes, subject to one important exception.
In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

10. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a “subject access request”.
All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 11. To make this as easy as possible for you, a Subject Access Request Form is available for you to use. You do not have to use this form, but it is the easiest way to tell us everything we need to know to respond to your request as quickly as possible.
There is not normally any charge for a subject access request. If your request is ‘manifestly unfounded or excessive’ (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.
We will aim to respond to your subject access request within 14 days and, in any case, not more than one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

11. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a

subject access request, please use the following details for the attention of The Data Protection Officer, Mr George Walton.
Email address: admin@kcts.me.uk
Telephone number: 01509 600330
Postal Address: Springfield Farm, Charley Road, Oaks in Charnwood, Leicestershire, LE12 9YA

12. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.
Any changes will be made available on our website:
www.kcts.me.uk

Subject Access Request Form

This form is for any person who wishes to apply for access to personal data held by KCTL only. Please read the Subject Access Request Guidance Notes below before completing this form. A separate form should be completed for each individual.

NOTE: This is not a mandatory form – Subject Access requests made in other formats will also be accepted but this form is designed to speed up the process.

Subject Access Request

Please read before filling in the Subject Access Request Form

Sections 1, 2, 3, 4 and 5 should be completed for all applications.

Section 3 (Proof of the applicant's identity) - If you do not have any of the forms of identity listed, we may in exceptional circumstances accept alternatives for consideration.

This form is designed to assist the process of making a subject access and, as a consequence, may speed the process up; but it is not mandatory, all subject access requests made in other formats will also be processed.

General Notes

1. We will not acknowledge your application in writing, but we will provide you with a reference number when we write to you.
2. Disclosure by post is usually made by first class post to the address you provide in section 2 or. We will also disclose by email where requested.

Checklist

Have you completed all relevant sections of the form?

Have you enclosed two pieces of identification from the lists in Section 3

(One from each of A and B)?

Have you signed the declaration in Section 5?

Have you provided as much information as possible to enable us to find the data you require?

Please send your completed form, proof of identity to:

Springfield Farm

Charley Road

Oaks in Charnwood

Leicestershire, LE12 9YA Email: admin@kcts.me.uk

Subject Access Request Form

Section 1 – Applicant Details

Title (please tick one):	Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Title (please state):
Forename(s):	
Family Name:	
Previous Family Name:	
Other name(s) known by:	
Date of Birth (dd/mm/yyyy):	……../……./……. Male ☐ or Female ☐
Place of Birth:	

Section 2 – Applicant Details

Current Address:	
Postcode	
Daytime Telephone No:	
Email Address:	
Previous Address:	
Postcode:	

Subject Access Request Form

Section 3 – Proof of the applicant's identity

In order to prove the applicant's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

Please DO NOT send an original passport, driving licence or identity card.

List A (photocopy of one from below)		List B (plus one original from below) *	
Passport/Travel Document	☐	A letter sent to you by KCTL	☐
Photo driving licence	☐	Utility bill showing current home address	☐
Foreign National Identity Card	☐	Bank Statement or Building Society Book	☐
Training Photo ID Card	☐		☐
	☐		☐
	☐		☐

Section 4 – Details of Information Required

Please use this space to give us any details about the information you are requesting, for example by stating specific documents you require (use extra sheets if necessary):

Section 5 – Declaration

The information which I have supplied in this application is correct, and I am the person to whom it relates or a representative acting on his/her behalf. I understand that the Her Majesty's Passport Office may need to obtain further information from me/my representative in order to comply with this request.

Signature of Applicant:	Date:

Timescale

If you have specific reasons for requiring data by a specific date, please give details below:

(a) Date required:
(b) Reason (please state and supply supporting evidence):

On completion of this request this form will be securely destroyed

Desktop Computers

Staff must log into the system using their own user ID and password. Logging in using someone else's script is a disciplinary offence, unless authorised to do so by a senior manager or director.

All data must be stored on the appropriate areas of the network, and files named in accordance with guidelines for each application or specific use of the software.

Data held on the network drives will be backed-up automatically by the IT department each night.

Personal files must not be held on any part of the computer system. Doing so will be a disciplinary offence.

Non-authorised applications, software or data must not be downloaded, held on any part of the computer system, local or network, this includes graphics, logo's etc. Downloading will be a disciplinary offence and where a virus or similar destructive or threatening software is involved grave misconduct will be presumed.

A deliberate attempt to access files and/or network areas for which authority has not been granted, will be a disciplinary offence.

Laptops, Notebooks and Other Portable Computing Equipment

Any portable computer issued to a member of staff remains the property of Keith Cook Training Limited and must be returned on termination of a contract of employment.

Portable computers are to be used solely for company business, in accordance with the acceptable use of the Internet and e-mail policy.

Restrictions for use of desktop computers apply equally to portable computer users.

Environmental Policy

Keith Cook Training Limited provides training in the use of a wide range of construction plant and recognises the potential for environmental damage relating to the use of plant and machinery.

We aim to meet, and whenever practical, exceed the requirements of legislation appropriate to our sector, and to minimise any adverse effects from our operations.

We aim to reduce pollution, emissions, and waste by operating plant as efficiently as possible, using approved fuels and lubricants and recycling waste where appropriate.

All potentially damaging waste will be disposed of responsibly in accordance with local government provision.

We aim to reduce our use of energy by switching off all electrical and/or electronic equipment when not in use.

Our training and assessment programmes will incorporate the potential impact on the environment from the operation of construction plant and suggest strategies for minimising damage to the environment.

Instructors and assessors will receive regular update training in environmental issues.

The effectiveness of this environmental policy will be reviewed annually by the Directors.

Quality Policy

The assessment centre will follow codes of good practice as published from time to time by the NVQ awarding and lead bodies, standards setting bodies, accrediting bodies, central and local Government agencies, and other appropriate authorities.

A system of eliciting and monitoring customer comments will be enforced for all training and assessment programmes. The resulting statistics will be published to all authorised personnel with the intent of constantly improving the quality of service offered to our candidates.

A procedure for processing customer complaints and ensuring customer satisfaction will be in force at all times.

Assessor performance will be monitored through the Internal Verification Procedures as required by the Awarding Body. The performance of all assessors is therefore monitored against A Unit Standards at minimum six monthly intervals.

All CPCS testing and training will be continuingly monitored through and in accordance with Company policies and procedures including random inspections of documentation.

Driver CPC training will be continuingly monitored through and in accordance with Company policies and procedures Terms and Conditions reference xxvii including random inspections of documentation.

Equality and Diversity Policy

Keith Cook Training Ltd is committed to eliminating discrimination and encouraging diversity amongst our workforces. Our aim is that our workforce will be truly representative of all sections of society and each employee feels respected and able to give of their best.

To that end the purpose of this policy is to provide equality and fairness for all in our employment and not to discriminate on grounds of their gender, age, sexual orientation, marital or parental status or other family circumstance, race, ethnic or national origin, colour, creed, disability, political belief, membership of, or activities as part of a trade union, social or economic class, or any other ground not relevant to good employment practice. We oppose all forms of unlawful and unfair discrimination.

All employees, whether part-time, full-time, or temporary, will be treated fairly and with respect. Selection for employment, promotion, training, or any other benefit will be on the basis of aptitude and ability. All employees will be helped and encouraged to develop their full potential and the talents and resources of the workforce will be fully utilised to maximise the efficiency of the organisation.

Our commitment:

• To create an environment in which individual differences and the contributions of all our staff are recognised and valued.
• Every employee is entitled to a working environment that promotes dignity and respect to all. No form of intimidation, bullying or harassment will be tolerated.
• Training, development, and progression opportunities are available to all staff.
• Equality in the workplace is good management practice and makes sound business sense.
• We will review all our employment practices and procedures to ensure fairness.
• Breaches of our equality policy will be regarded as misconduct and could lead to disciplinary proceedings.
• This policy is fully supported by senior management and has been agreed with trade unions and/or employee representatives. (Insert details if appropriate).
• The policy will be monitored and reviewed annually.
• We will implement the intentions in this policy via an annual action plan.

Customer Service Policy

Policy Statement

Keith Cook Training Limited will strive to delight customers by promoting a professional and courteous image through ensuring that all projects are completed on time, on budget and to agreed quality standards, first time, every time.

Customer Service Targets

- Telephones will be answered within five rings.
- Requests for information which can be satisfied with a standard letter and appropriate leaflets and/or forms will be answered:
    - Requests received before 1:00 pm - despatched last post same day.
    - Requests received after 1:00 pm - despatched first post next working day.
- All staff will have sufficient product and service knowledge to be able to respond personally to first line requests for information and to signpost enquirers to the appropriate specialist within the team.
- All telephone messages will be noted and passed to the appropriate person with minimal delay.
- Where delay is inevitable, the enquirer will be contacted and informed of the reasons for delay in response.
- Meetings with potential or actual customers will be noted during the meeting and acknowledged on return to the office or within 48 hours whichever is the shortest interval.
- Quotations will be provided by the date agreed with the potential customer, or a written reason for delay will be provided.
- Orders will be acknowledged on receipt.
- Regular communication will be maintained with customers throughout the duration of all projects.
- Compliments received from customers, whether in writing, via requested feedback or via the telephone or other verbal means, will be recorded by the Centre Manager and reported to Keith Cook and to the individual so complimented.

Customer Complaints Procedure

To include staff, tutor, client, and delegate

1. Any complaints, however received, from customers, staff, tutors, or clients concerning the quality of service or product provided by Keith Cook Training Limited will be referred immediately to the centre manager.
2. A record of complaints received, the reason for the complaint, and the solution will be maintained, and statistics derived from the records used to improve products and services.
3. Any adverse comments made by staff, tutors or delegates on training course assessment forms will be regarded as a complaint and recorded accordingly.
4. Any delegates or tutors awarding ‘poor' to any aspect of a training course on the assessment form, will be regarded as a complaint, and recorded accordingly.
5. All complaints will be investigated, and a report provided to the Centre regardless of the severity of the incident or potential impact on business.

6. An acknowledgement of the complaint will be sent to the customer on the day on which the complaint is received.

7. The Centre will instigate an investigation into the cause of the complaint. The investigation may be undertaken personally by the Centre or may be delegated to an appropriate and independent member of the assessment team.

8. The Centre Management team will discuss the complaint and its cause(s) and review procedures in order to prevent a similar complaint arising.

9. The customer will be advised of changes arising as a result of the complaint.

10. The customer will be offered compensation only when it is deemed appropriate by the Directors.

11. All complaints must be submitted in writing to KCT's Main office within 10 working days.

Conflict of Interest Policy

CONFLICTS OF INTEREST POLICY

No member of KCTL Training Board of Directors or Staff shall derive any personal profit or gain, directly or indirectly, by reason of his or her participation with KCTL Training. This shall also include the member's business or other non-profit affiliations, family and/or significant other, employer, or close associates who may stand to receive a benefit or gain. Each individual shall disclose to the Company Manager any personal interests which he or she may have in any matter pending before the organization and shall refrain from participation in any discussion or decision on such matter.

In addition, any member of KCTL Directors or Staff shall refrain from obtaining any list of clients or donors for personal or private solicitation purposes at any time during the term of their affiliation.

Any new member of the Board of Directors shall be given this policy at the time of their election onto the Board of Directors and the policy will be reviewed annually by the board at a regularly scheduled meeting.

We understand that the purposes of this policy are to protect the integrity of Organization Name and the organization's decision-making process as well as to enable our constituencies to have confidence in the integrity, intentions and actions of the officers, staff, board members and volunteers. To that end, we understand that this policy is not meant to supplement good judgment and all constituents should respect its spirit as well as its wording.

If a conflict of interest is identified, contact the appropriate awarding or accrediting body to request an EQA to attend on an agreed date and time for testing, this action would mean that testing could take place with the test being externally quality audited. If this process cannot be completed then recommend that the test be completed at another centre.

Appeals CPCS Testing Taken from Scheme Booklet

7.6 Appeals
There are two types of disputes that a CPCS Test Centre can lodge an appeal:

7.6.1 Appeal against a Sanction for non-compliance:
In the event of a dispute regarding a sanction for non-compliance with Scheme Rules, a CPCS Test Centre must lodge an appeal in writing, within 10 Normal Working Days of the receiving written notification. The appeal must be sent to either the North or South Team Leader at:

CPCS Quality Assurance
NOCN Job Cards
PO Box 1242
Kings Lynn
Norfolk
PE30 9FQ (Note this is not the correct address and will be amended when informed)

If no appeal is made within 10 Normal Working Day appeal period action to implement the suspension or termination of accreditation will be taken.

In the event that an appeal is made within the 10 Normal Working Day appeal period, no action to implement the suspension or termination will be made until the appeal has been heard and the outcome of the Appeals Process has been determined.

7.6.2 Appeals against Test Centre Scheme Rules:
In the event of a dispute regarding Scheme Rules, a CPCS Test Centre must lodge and appeal in writing. The appeal must be sent to:

CPCS Quality Assurance
NOCN Job Cards
PO Box 1242
Kings Lynn
Norfolk
PE30 9FQ

The CPCS Department will provide full details of the Appeals process on request.

Appeals for Accrediting Bodies

All delegates will be provided with a copy of the Awarding Body appeals procedure on request which may be invoked should the following procedure fail to bring a successful end to an appeal.

In the event of any delegate being dissatisfied with the performance, decision or conduct of an instructor/Trainer or Tester, they should: -

1. Contact the Centre Manager and explain, in detail, the nature of their complaint.
2. The centre manager will record the complaint in detail, and, working with a director of the company, investigate the cause of complaint.
3. The centre manager and director will meet with the instructor/Trainer/Tester to discuss the complaint in detail. The centre manager will record the discussion and all decisions reached.
4. The centre manager and/or director will suggest a solution to the candidate, which may include an additional training/testing by an alternative member of staff. The solution will be recorded together with the delegate's reply to the solution.
5. Should the delegate reject the solution offered by the centre manager, the Accrediting Body appeals procedure may be invoked, subject to the candidate paying such fees as may be demanded by the Awarding Body.

Appeals (Qualification Candidates)

All candidates will be provided with a copy of the Awarding Body appeals procedure which may be invoked should the following procedure fail to bring a successful end to an appeal.

In the event of any candidate being dissatisfied with the performance, decision or conduct of an assessor or internal verifier, they should: -

1. Contact the Centre Manager and explain, in detail, the nature of their complaint.
2. The centre manager will record the complaint in detail, and, working with a director of the company, investigate the cause of complaint.
3. The centre manager and director will meet with the assessor/internal verifier to discuss the complaint in detail. The centre manager will record the discussion and all decisions reached.
4. The centre manager and/or director will suggest a solution to the candidate, which may include an additional assessment/verification by an alternative member of staff. The solution will be recorded together with the candidate's reply to the solution.

5. Should the candidate reject the solution offered by the centre manager, the Awarding Body appeals procedure may be invoked, subject to the candidate paying such fees as may be demanded by the Awarding Body.

6. Learners of regulated qualifications have the right to complain to SQA Accreditation or Ofqual if they have exhausted KCTLs and the relevant awarding organisation procedure.

   www.sqa.org.uk or www.gov.uk/government/organisations/ofqual

WHISTLE BLOWING POLICY

STATEMENT

Employees are often the first to realise that there may be something seriously wrong within Keith Cook Training Ltd However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the company. They may also fear harassment or victimisation. In these circumstances, it may be easier to ignore the concern rather than report what may just be a suspicion of malpractice.

Keith Cook Training Ltd is committed to the highest possible standards of openness, probity, and accountability. In line with that commitment, we encourage employees and others with serious concerns about any aspect of the organisation's work to come forward and voice those concerns. It is recognised that certain cases will have to proceed on a confidential basis. This policy document makes it clear that employees can do something without fear of reprisals. This Whistle blowing Policy is intended to encourage and enable employees to raise serious concerns **within** the company rather than overlooking a problem or blowing the whistle outside.

AIMS & OBJECTIVES

This policy aims to:

- provide avenues for you to raise concerns and receive feedback on any action taken.
- allow you to take the matter further if you are dissatisfied with the Council's response;
- Reassure you that you will be protected from reprisals or victimisation for whistle blowing in good faith.

ADDITIONAL INFORMATION

This policy should be read in conjunction with Whistle Blowing Guidance (document WBG1).

RESPONSIBILITY

The Senior Quality Manager has overall responsibility for the maintenance and operation of this policy and maintains a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality).

Verified: George Walton Position: Managing Date: 03/01/2024

Refuelling Procedures

ICE Plant, ICE Lift Trucks

1. DO NOT smoke or permit any open flame in area while you are servicing fuel system.
2. Be sure hose nozzle is grounded against filler tube during refuelling to prevent static electricity; failure to follow this warning may result in injury to personnel or equipment damage.
3. Operating personnel must wear fuel resistant gloves when handling fuels, if exposed to fuel promptly wash exposed skin and change fuel-soaked clothing.
4. Place portable fire extinguisher within reach prior to refuelling.

5. DO NOT overfill tank, if fuel starts foaming from fuel tank, stop immediately to avoid fuel spillage.
6. Failure to follow these warnings could result in injury or death to personnel.

   a. Shut down engine.
   b. Wipe off dirt on and around filler cap.
   c. Unlock filler cap and open.
   d. Refuel tank. DO NOT overfill tank.
   e. Close filler cap and lock

Handheld Engine Tools

1 Stop the engine and, if necessary, allow cooling before refuelling.
Petrol vapour is invisible and can travel considerable distances from spillage or fuelling sites. Maintain a safe distance from all sources of ignition at all times.

2 Store fuel to avoid vapor ignition from any source such as fires, people smoking or the equipment. Select a site shaded from direct sunlight and away from watercourses and drains.

3 Containers must be clearly labelled and have securely fitting caps. Plastic containers must be designed and approved for use with petrol or diesel fuel.

4 Replace the fuel cap securely.

5 Keep fuel from contacting the skin. If fuel gets into the eyes wash out with sterile water immediately and seek medical advice as soon as possible.

General Booking Procedures

KCT has a number of booking procedures in place for the various accrediting/awarding organisation the company is registered to the following procedure is generic and depending on the AO's may have further details within these P & Ps.

1. Contact
2. Information Advice & Guidance (IAG)
3. Costs explained.
4. Availability
5. Agree Dates and Hold in the KCT Diary
6. Booking Form/s emailed/mailed out Diary updated and highlighted in yellow.
7. Diary amended on receipt of Booking Form to Confirmed
8. Confirmation of names attending on the day of training

Part 6 – Awarding & Accrediting Bodies additional policies requirements.

Safeguarding Vulnerable Adults

Procedures and Guidance

Contents

1. Introduction

2. Purpose of the procedures and guidance

3. When to invoke the procedures

4. Process

5. Responding to telephone reports of abuse

6. Assessing the need for immediate action

7. Out of hours concerns

8. The initial assessment – within 24 hours

9. Referrals to Adult Care Social Services

10. Making decisions/taking action

11. Public Guardian investigations

12. Sharing information with others

13. Action following a Public Guardian investigation

14. Crime

15. Records and reporting

Safeguarding Appendices:

1. Process for action in response to suspected or alleged abuse.

2. Proforma for gathering information about an allegation of abuse.

3. Information sharing protocol.

4. Glossary

Safeguarding Vulnerable Adults Procedures & Guidance

1. Introduction

1.1 This document supports the *Safeguarding Vulnerable Adults Policy*. It outlines procedures and timescales to be followed in response to allegations, suspicions or reports of abuse of a vulnerable adult, and provides guidance to staff. It should be read and applied in conjunction with the *Safeguarding Vulnerable Adults Policy* and the *Protocol for joint work between the Office of the Public Guardian and Local Authorities for Safeguarding Vulnerable Adults.*

1.2 The OPG strives, through its safeguarding adult's policy and procedures, to ensure that vulnerable adults receive their entitlement to safeguards that:

• Prevent abuse from occurring and/or continuing where possible

• Identify abuse promptly

• Ensure the abuse ceases and the perpetrator is dealt with wherever possible

• Undertake to notify Local Authorities/Police and other appropriate agencies when an abuse situation is identified.

It will do so by carrying out its statutory duties, and by thoroughly investigating reported concerns about the conduct of Deputies and registered Attorneys.

1.3 For definitions of vulnerable adult and abuse, refer to the *OPG Safeguarding Vulnerable Adults Policy*. A glossary of terms is also provided in Appendix 4 of this document.

1.4 References to "staff" throughout this document should be taken to include permanent and temporary staff, agency staff, Court of Protection Visitors and Contractors engaged in OPG business.

2. Purpose of the procedures and guidance

2.1 The overall purpose of these procedures and guidance is to equip staff to respond promptly and appropriately to suspicions, allegations, or reports of abuse. It applies to all those engaged in OPG business and details:

• When to invoke the safeguarding vulnerable adult's procedures

• The process to follow

• Timescales

• The assessments and information needed at each stage in the process

• Who to refer to and who can provide advice

• When to refer to external agencies

2.2 Any member of staff, not just those in client facing roles, could identify a suspicion, report, or allegation of abuse of a vulnerable adult and has a responsibility to follow these procedures.

3. When to invoke the procedures

3.1 Staff should firstly ensure they are familiar with the definitions of vulnerable adult, and the role of the OPG in safeguarding, outlined in the *Safeguarding Vulnerable Adults Policy*. The policy also outlines potential alerts to abuse, but it should be recognised that abuse takes many forms and can be perpetuated by anyone, including staff or other vulnerable adults.

3.2 Information about potential abuse may come from evidence or from any individual, for example:

• A client

• Deputy

• Attorney

• Relative or friend, or a third party e.g., a neighbour

• Member of staff

• A provider or a commissioner of services

• Court of Protection Visitor

• OPG staff (from information found in the client records)

• Other agencies such as Court Funds Office, Adult Care Social Services, the Police, Solicitors Regulation Authority, CSCI

3.3 Information may be found in or received by:

• Phone

• Court Order (ordering an investigation or report from the Public Guardian)

• Letter or document

• Email

• Visit report

• On an OPG form, including a report form, complaints form.

3.4 To avoid delays in responding to abuse, it is important to check incoming post, emails and forms daily and prioritise those that contain information about potential abuse.

3.5 A suspicion of abuse doesn't have to come from an informant. It can be an opinion formed by a staff member or visitor, e.g., if an unusual withdrawal is seen on a bank statement, or there is a sudden unexplained ability to pay fees.

3.6 These procedures should be invoked for any suspicion, allegation, or report of abuse.

4. Process

4.1 When a suspicion, allegation, or report of abuse of a vulnerable adult comes to light, then staff should follow the process flow chart in Appendix 1. This detail the process to raise an alert, the timescales involved and possible responses to the concern.

4.2 In all cases, the alert should be passed to the Compliance and Regulation team who will assess the urgency of the situation and who should respond. Where the concern relates to a client with a Court appointed Deputy who is subject to close supervision (Type 1 supervision), the team to respond will be the Supervision Casework team. In all other cases, the Compliance and Regulation team will respond.

4.3 If the alleged abuse is by a member of staff, contractor or Court of Protection Visitor, the relevant Head of Division and the Head of Finance and Resources must be informed, and HR and Fraud response policies will be followed.

4.4 The abuse alert proforma in Appendix 2 should be completed in all cases and passed **on the day the suspicion, allegation or report is received** to the Compliance and Regulation team together with any documentation prompting the concern (e.g., letter, bank statement). The form is intended for use by staff throughout the OPG to alert the Compliance and Regulation team to potential abuse. If the report or suspicion of abuse arises within any of the Supervision teams, then staff in these teams should still complete the form to initiate the safeguarding process.

4.5 Court of Protection Visitors who suspect or find evidence of abuse in the course of a visit should report it to the OPG on the abuse alert form within 24 hours and file the visit report as soon as possible thereafter. If it appears that someone is in immediate danger, the Visitor should contact the relevant emergency services and/or the local safeguarding/adult protection team. Section 7 details how to deal with out-of-hours concerns.

4.6 At each stage of the process, the aim is to:

• Establish the facts

• Assess the needs of, and risks to, the client (vulnerable adult) for protection, support, and redress

• Make decisions with regards to follow up action that needs to be taken in order to protect the adult and with regards to the (suspected) perpetrator

5. Responding to telephone reports of abuse

5.1 Contact Centre staff will often be the first point of contact for a person reporting concerns about abuse by telephone, although information may be received by any other area of the business. Someone reporting abuse by telephone may be distressed or nervous, and the initial contact is often critically important. It is important to listen carefully, record what is being said, and avoid asking any leading questions.

5.2 Information from an initial contact by telephone should be collected using the pro-forma in Appendix 2. When recording the caller's information, follow the procedures listed below:

1. Ensure that you obtain details of the client/vulnerable adult: their name; contact details; date of birth; gender; any language or communication needs they have.

2. Check to find out if the vulnerable adult is an OPG client.

3. If possible, find out whether

a. Adult Care Social Services

b. any other agencies are already involved with this client. It is helpful to know if any other agencies have been informed of the concern or if it has been reported to the police, although you should not recommend any action to the complainant without discussing it with a manager.

4. If possible, determine whether the information you are receiving is an allegation or a suspicion or if there is actual clear evidence of abuse (e.g., witnessed behaviour).

5. If possible, determine if this is the first concern or if there have been previous suspicions or actual abuse.

6. If possible, determine what sort of abuse you are being informed about, whether it is a 'one off' incident or possibility of ongoing abuse, who the alleged perpetrator is and what degree of contact they have with the client. Care needs to be taken that only the basic information is gathered at this stage and not a detailed 'interrogation' of the person making the allegation, so that no future police investigation (if it becomes necessary) is prejudiced.

7. Obtain the contact details of the person making the allegation and their relationship to the client (telephone number/ email or some other method of making contact of the informant is necessary should more information be needed). Note that some people may wish to remain anonymous, but this should not prevent you from recording the details of the allegation or suspicion of abuse.

8. Obtain the informant's consent to pass the information on to the relevant section of the OPG

9. Thank the informant for making the disclosure. Explain that it will be processed through the safeguarding vulnerable adult's procedures and will be treated seriously and with urgency. Explain how the safeguarding procedures and policy can be obtained if they want more information. Be as clear as you can with them what will happen next as a result of their allegation.

Whistleblowing

A whistle-blower is someone who voices concerns, sometimes about the practices of an organisation or an individual member of staff. Sometimes whistle-blowers decide to do so anonymously, which can make the investigation difficult. The OPG promotes and support openness in order to protect vulnerable adults, and so whistle-blowers should always be:

- Treated seriously.
- Treated confidentially where relevant.
- Treated in a fair and equitable manner.
- Kept informed of action taken and its outcome.

6. Assessing the need for immediate action

6.1 The first priority is to ensure the safety of the individual. If it appears that someone is in immediate danger, the relevant emergency services should be contacted, e.g., police, ambulance. A senior manager should be consulted, if possible, but this should not delay acting.

6.2 Where it seems that the vulnerable adult is not in immediate danger but there is a need for a swift response the details should be passed **immediately** to the Compliance and Regulation team so that they can assess the situation. This will be a matter for judgement in each case, but where possible, there should be no delay in highlighting the situation.

The following are examples of serious concerns that justify a swift response:

• There is reason to believe someone is in danger

• There is reason to believe that major injury or serious physical or mental ill health may result

• The incidents are increasing in frequency

• The incidents are increasing in severity

• The behaviour is persistent and/or deliberate

6.3 In all cases, the alert form and details must be passed to the Compliance and Regulation team **on the same day** as the situation comes to light.

7. Out of hours concerns

7.1 Where concerns arise out of normal office hours, for example, during overtime, the most senior manager available will make a decision on whether there is a need for immediate action. This may involve contacting the Police or the Local Authority emergency duty team in the vulnerable adults' local area for advice. Contact details can be found on the relevant Local Authority or Police authority website.

7.2 Where an out of hours' concern is raised by a Court of Protection visitor, e.g., during an evening or weekend visit, the Visitor should decide whether the situation is such that there is a need to contact the Police or Local Authority emergency duty team. The abuse alert pro-forma should be completed as soon as possible with details of any immediate action taken and passed to the Compliance and Regulation team at the start of the next working day.

8. The initial assessment – within 24 hours

8.1 A member of the Compliance and Regulation team will carry out the initial assessment. This investigation should take place within 24 hours of the concern being raised.

8.2 The initial assessment will follow the process for investigations in the investigations manual and is summarised in this procedure.

8.3 The purpose of the initial assessment is to assess the level of risk and to determine the urgency and priority of the situation. It may be necessary to contact others for more information before making this decision.

8.4 Factors to consider when assessing the level of risk include.

• Factors in the situation which could increase vulnerability, including:

- Environmental factors – does the vulnerable adult live alone or only with alleged perpetrator?

- Communication

- Financial factors

- The existence of social and cultural networks and support – are there others who provide care to the vulnerable adult?

• The nature and extent of the abuse – is it a “one-off” incident or an ongoing problem (although isolated incidents can still constitute an emergency).

• The length of time over which the abuse has been happening

• The impact on the individual

• The impact on others

• Whether the situation can be monitored.

8.5 If the case is subject to Type 1 supervision, there must be liaison with the Supervision casework team at this stage to ascertain current casework activity, and to inform the assessment and agree responsibility for taking the matter forward.

8.6 Any enquiries to external agencies at this stage must be made carefully and sensitively, in order not to prejudice any Police investigation and to avoid increasing the risk to the vulnerable adult. Where appropriate, contact should be made with the vulnerable adult’s existing social worker, if there is one, or otherwise with the Adult Care Social Services or Safeguarding Adults/Adult Protection team of the relevant Local Authority.

8.7 Although all cases should be treated as important, this assessment will help to determine whether action needs to be taken immediately i.e., the same day (for example, if an emergency application to Court is needed to freeze bank accounts), or whether you can afford to take longer to take action if more information needs to be gathered. The assessment should also specify any early input required to reduce the level of risk.

8.8 If there is immediate risk to the vulnerable adult or if there is evidence that a criminal offence (see section 14) may have been committed, the Police should be contacted. Whether to involve the Police will be a matter for the Team Manager and Head of Supervision or another Executive team member. This may involve a discussion with Adult Care Social Services and with the OPG Legal Advisor, as it will not always be clear-cut. However, seeking such advice should not delay taking urgent action where the safety of a vulnerable adult is at risk. .

8.9 The initial assessment will also determine whether the OPG has powers to investigate further (see Section 11) and/or whether the matter will be referred to the local Adult Care Social Services for them to initiate their safeguarding procedures. There does not have to be proof of abuse for a referral to Adult Care Social Services to be made.

8.10 Court of Protection administration staff must be alerted at this stage to any concerns that may affect pending court applications, for example, if the alleged perpetrator is a professional deputy who may have other applications pending. This is done by notifying the Manager of the New Applications team.

8.11 The response and subsequent priority given to an investigation will be based on an assessment of the seriousness of the situation and whether there is an ongoing risk to the client and others. The table overleaf sets out a framework for considering urgency and risk and presents clusters of factors and responses to those factors. However, it should not be used as a rigid framework without full and detailed examination of the case. The Compliance and Regulation or Supervision Casework team manager should discuss the appropriate response with colleagues and allocate resources accordingly. **Factors**	**Response**
A: Appears to involve the following: • Institutional abuse • A number of people have been adversely affected • A number of criminal offences may have been committed	Complex investigation including Adult Care Social Services and Police. A comprehensive action plan and full investigation should be undertaken. Sufficient resources should be allocated with Senior Management support to manage, co-ordinate and investigate. **High priority**.
B: Appears to involve the following: • The financial, physical, psychological, or emotional well-being of the client has been adversely affected by the alleged incident • A criminal offence may have been committed • Possible breach of professional Code of Conduct • Actual or potential risk of harm or exploitation to other people at risk • Deliberate intent to exploit or harm the client • Significant breach of implied “duty of care” • The referral forms part of a pattern of abuse against an individual	Suggests a case with a serious impact on a vulnerable adult, possibly with implications that go beyond the individual. A criminal offence is likely to have been committed. A comprehensive action plan and full investigation should be undertaken, and sufficient resources allocated to this. **High priority.**
C: Appears to involve the following: • The financial, physical, psychological, or emotional well-being of the client may be being adversely affected. • The concerns reflect difficulties and tension in the way services are being provided to the client or decisions are being made on behalf of the client	The action plan and investigation should assess the seriousness of the case and the impact on the client at risk, taking full account of any past incidents or suspicions. Targeted support and monitoring may be considered. **Medium Priority**

• The concerns reflect difficulties and tensions within the network of informal support provided to the client (e.g., perceived difficulties between the client and family/friends) • Concerns have occurred in the past, but at lengthy and infrequent intervals	
D: Appears to involve the following: • A possibly isolated incident that appears to have had little or minimal impact on the financial, physical, psychological, or emotional well-being of the client • Not obvious part of a pattern of abuse • No clear criminal offence • No clear intent to harm or exploit the client	The action plan and investigation should include an assessment of the seriousness of the event or incident. **Low Priority.**

9. Referrals to Adult Care Social Services

9.1 For information about referrals to Adult Care Social Services see the *Protocol for Joint Work between the Office of the Public Guardian and Local Authorities for Safeguarding Vulnerable Adults.* Where a referral is made, Adult Care Social Services or the department leading the investigation may call a case conference or strategy planning meeting in line with their own policy, practice, and procedures.

• *Every Local Authority has a* ***Safeguarding Co-ordinator,*** *who sets and monitors local policies and procedures, and provides expert advice.*

• *Every Local Authority has a* ***central contact point*** *for receiving safeguarding alerts.*

• *For each case, a* ***safeguarding investigator*** *will be designated.*

10. Making decisions/taking action

10.1 Following the initial assessment, a decision must be made as to the agreed course of action in line with the following considerations:

• Whether the Public Guardian has statutory authority to conduct an investigation (see section 11), and if so, which team and which worker will lead the investigation.

• Whether any suspicion or allegation should be communicated to the client's local Adult Care Social Services safeguarding adults/adult protection contact so agreement can be made as to how to progress with an investigation.

• Whether responsibility for investigation of the abuse (beyond the simple gathering of information) will be passed onto Adult Care Social Services or, where a crime is felt to have been committed, to the Police or other agency if this is considered appropriate. Whichever agency is leading on a case, OPG staff need to ensure that the agency will keep the OPG informed as to the progress of the case and share the conclusion of any investigations/intended action which may impact upon the OPG, its clients, Deputies or Attorneys.

• Whether the abuse is considered to be a criminal offence, in which case the Police should be involved. Whether to involve the police will be a matter for the Team Manager and Head of Supervision, or another Executive team member. This may involve a discussion with Adult Care Social Services and with the OPG Legal Advisor, as it will not always be clear-cut, but should not delay any referral to the Police.

10.2 If the vulnerable person is not a client of the OPG (i.e. does not have an appointed Deputy, or is subject to a Court of Protection Order authorising someone to carry out a transaction, or is the donee of a registered power of attorney), a member of the Compliance and Regulation team should contact the relevant Adult Care Social Services, or the relevant Police Force if a criminal offence is suspected, and all information concerning the suspicion or allegation discussed with/passed onto them. The details of the person at risk and the alleged perpetrator of the abuse should be retained by the Compliance and Regulation Manager and passed to the Court of Protection administration team (via the Manager of the New Applications team) in case an application is in progress or may be made at a later date.

11. Public Guardian investigations

11.1 The Mental Capacity Act 2005 gives the Public Guardian authority to investigate in the following circumstances:

• Where the concern is about the actions of a Deputy appointed by the Court of Protection

• Where the concern is about the actions of a donee of a registered power of attorney (EPA or LPA)

• Where the concern is about a transaction carried out under a single order from the Court of Protection.

11.2 The Public Guardian does **not** have statutory authority to conduct investigations in the following scenarios and the Compliance and Regulation team should refer to another agency or advise as detailed below.

• Concerns about the actions of Attorneys acting under an unregistered EPA

In this scenario, a referral should be made to Adult Care Social Services for an investigation under their procedures which will determine how to continue. If the donor of the EPA lacks capacity to make decisions, the advice may be that an application is made to the Court of Protection for revocation of the EPA and the appointment of a Deputy. The Court will sometimes order the Public Guardian to provide a report under Section 49 of the Mental Capacity Act in such cases, which will come to the Compliance and Regulation team for action. If the donor of the EPA has capacity, then consideration should be given to suggesting that a local agency/solicitor or third party helps her/him decide whether to revoke the EPA and make an LPA.

• Concerns about the actions of persons acting under certain types of Court of Protection Short Orders

Short Orders were granted by the Court of Protection prior to implementation of the Mental Capacity Act in October 2007. The Public Guardian does not have powers to investigate all short order scenarios. Short order “applicants” (as the person acting was known) were not converted to Deputies by the Mental Capacity Act and therefore the Public Guardian does not have legal authority to investigate complaints. However, it may be possible for the OPG to investigate single transactions that were authorised by way of short order. Advice should be sought from the Legal Adviser if in doubt. Where there is no authority to investigate, a referral should be made to Adult Care Social Services for an investigation under their procedures which will determine how to continue and/or advise that an application is made to the Court for Protection for revocation of the Order, and if, necessary, for an Order appointing a Deputy. The application could include authority to investigate the transactions of the person acting under the Short Order.

• Concerns about the actions of former Receivers or Deputies

Where there are concerns about the actions of a former Receiver (i.e., someone whose appointment was terminated prior to 1 October 2007) or a Deputy whose appointment has terminated, the advice should be that this is a matter for the current Deputy, if there is one, to deal with. This includes scenarios where the former Receiver or Deputy has died. If the Court of Protection terminates a Deputyship due to concerns about the actions of the Deputy, the Court may order any new Deputy who is appointed to investigate the former Receiver or Deputy. Sometimes concerns arise after the vulnerable adult has died. Any Deputyship terminates on death, and it falls to the vulnerable adult’s personal representatives to deal with any investigation.

Where a Deputy has been discharged, or has died, or the vulnerable adult has died, the OPG can call for a final report from the former Deputy (or the personal representatives if the Deputy has died). This will be the responsibility of the Supervision team who are handling the enquiry. If the Public Guardian is not

satisfied, he may apply to the Court of Protection for enforcement of the security bond. This only applies to deaths/discharges after 1 October 2007.

• Concerns about the actions of third persons other than Deputies and Attorneys

In this scenario, a referral should be made to Adult Care Social Services for an investigation under their procedures which will determine how to continue. If the vulnerable adult has an appointed Deputy, then the Supervision team handling the enquiry should request that the OPG are kept informed of the situation. Consideration should be given to placing the case into Type 1 supervision so that the situation can be monitored through supervision of the Deputy and visits to the vulnerable adult from a Court of Protection Visitor.

• Concerns about persons acting under an appointee ship made by the Department of Work and Pensions (DWP)

In these circumstances, details should be passed to the Department for Work and Pensions and to Adult Care Social Services for investigation under their procedures.

11.3 The process and guidance for investigations carried out on behalf of the Public Guardian is set down in the Investigations Manual. It involves:

• agreeing an action plan with the section manager.

• carrying out the investigation

• completing a Section 58 report with recommendations, for consideration by the Public Guardian.

11.4 There are Key Performance Indicators (KPIs) that determine the timescales for completion of the action plan and investigation. These are published in the OPG's business plan and on the website. The initial assessment will determine the priority of the investigation against other ongoing investigations.

11.5 Where the Court of Protection has ordered an investigation or report under Section 49 of the Mental Capacity Act, the same process is followed, but the Court determines the timescale.

12. Sharing information with others

12.1 Understanding when and how to share information is critical when working with sensitive and personal information. The principle is that – wherever abuse is alleged or suspected – information should be shared between relevant professionals in exploring how to protect the allegations of abuse and their families and carers have a right to expect that confidences will be respected, and their privacy protected. But where their "vital interests"[1] (that is questions of life or death), "best interests",[2] or the public interest are involved, establishing the facts through information sharing takes precedence.

12.2 Investigating and responding to suspected abuse or neglect often requires close co-operation between organisations. Safeguarding will involve sharing personal information both about someone who is alleged to have experienced abuse and an alleged perpetrator.

12.3 Information can be shared in certain circumstances with other people or agencies in compliance with the GDPR 2018. Data can be shared with third parties "in the vital interest of the data subject" or "in the public interest". (E.g., in the interests of the client or others in the same care setting). Examples of when this may be appropriate will be if there is a need to seek information from another agency, or there is a potential risk to others from the alleged abuser. Any information relating to the accusation/suspicion of abuse should and can be shared with the Adult Care Social Services department or Police investigating the case.

12.4 There are specific provisions in the Mental Capacity Act 2005 that facilitate the sharing of information between the OPG, and local authority Adult Care Social Services departments and other agencies involved with the client's care or treatment. Section 58(2) provides for the Public Guardian's duties to supervise deputies and investigate concerns about the way a deputy or attorney is exercising their powers to be discharged "in co-operation with any other person who has functions in relation to the care or treatment of P". Additionally, Section 58(5) of the Mental Capacity Act 2005 gives the Public Guardian authority, in the course of carrying out his duties, to examine and take copies of any record of, or held by, a local authority and complied in connection with a social services function, so far as the record relates to P. This authority does not extend to records relating to a deputy or attorney.

12.5 If personal or sensitive information is to be shared, this should be done where possible with the person's agreement, after reasons have been explained. Consent may be verbal or written. If verbal, it should be recorded on the case file by the person handling the investigation or enquiry. If consent is not given, assessment of best interests may still justify further enquiries, while questions involving the public interest may justify overriding the person's views. Where adults lack capacity to safeguard themselves, others will need to make decisions for them in accordance with the Mental Capacity Act Code of Practice of alleged perpetrators of abuse must also be respected.

12.6 Any information shared should be on a "need to know" basis, i.e., only information that is directly relevant to the investigation, and the minimum necessary to achieve the objective of protection of vulnerable adults. Care must be taken to ensure the quality of the information shared, e.g., names, addresses and dates of birth are accurately recorded.

12.7 The information sharing protocol between the OPG, and Local Authorities is in Appendix 3. There is also guidance on *"Information assurance and security*", available on the OPG intranet. Hard copies are available for staff and Court of Protection Visitors who do not have access to the intranet. Staff should seek advice, when necessary, from the Records Manager, being mindful that it may be particularly important to share information for the protection of other possible abuse victims (e.g. in the case of a client living in a care home and being abused by a member of staff).

12.8 Before information is shared with the client's relatives or carers or the deputy/attorney careful consideration needs to be made as to the impact on the client of them holding that information e.g., will it put the client at further risk? A discussion with the local Adult Care Social Services safeguarding adults/adult protection contact may be appropriate in order to agree the best way forward.

12.9 Where Adult Care Social Services are leading the investigation, they may call a case conference or meeting. An OPG member of staff can be nominated by the Head of Supervision to attend that conference or meeting. A decision may be made not to send anyone to a case conference e.g., where the OPG involvement has been minimal or where the distance to travel is not felt to be an effective use of time. In these cases, any relevant information should be provided to the chair of the case conference beforehand and a request made for minutes.

12.10 When someone has reported concerns to the OPG, they often wish to know the outcome of any investigation. Consideration should be given to data protection requirements before sharing any information. It may not be possible to share the details of any investigation involving third parties. Where necessary, advice from the OPG's legal adviser should be sought. However, the informant should always be told when the OPG's action has completed, or when the matter has been referred to another agency for investigation, and who it has been referred to. Feedback must also be given to Court of Protection Visitors who raise an abuse alert.

13. Action following a Public Guardian investigation

13.1 At the end of a Public Guardian investigation, a decision will be made by the Public Guardian (or Head of Supervision in his absence) as to what action to take in relation to its responsibilities to the client. This may be a decision to make an application to the Court of Protection to remedy a situation or protect a client (for example, applying for the discharge of a Deputy and call in a security bond) and/or refer to the Police if information has emerged in the course of the investigation that suggests a crime may have been committed. Alternatively, a decision may be made to await the outcome of any Safeguarding Adults/Adult Protection or criminal investigation.

13.2 When considering if there has been abuse, all cases will be decided on the balance of probabilities, i.e., whether it is more likely than not that abuse has occurred. If the matter is criminal in nature this will be considered by the police to a higher standard of proof, which is that beyond reasonable doubt that abuse has occurred.

13.3 If the situation remains unclear but there is considered to be a risk of abuse, or there is considered to be a need for ongoing monitoring, Deputyship cases will be allocated to close (Type 1) supervision and the situation will be regularly reviewed. The supervision case worker must ensure that the management plan reflects this, e.g., by more frequent visits and contact with third parties. This level of supervision will remain during the period of the court order, except where the perpetrator of abuse is known and is removed from any contact with the client (or their access is *very* strictly controlled and monitored by Adult Care Social Services). Even if the alleged abuser is removed from his/her position as Deputy it may be

necessary to keep the case subject to close supervision if the casework team consider it continues to require monitoring.

13.4 The Court of Protection New Applications team will have been informed of any concerns and ongoing investigations into a Deputy and will alert the OPG to any pending applications by that Deputy. In that case, consideration will be given by the manager of the supervision team to whether it is necessary to make an application for the Public Guardian to be joined as a party to the proceedings.

13.5 If only a Finance and Property Deputy is in place, consideration must also be given to whether there should also be an application to appoint a Welfare Deputy in order to safeguard the client's wellbeing, possibly by the Finance and Property Deputy or by a third party.

14. Crime

14.1 If there is a possibility of a criminal offence having occurred, then it must be reported to the Police. Examples of when action may be considered a criminal offence include assault, whether physical or psychological, sexual assault and rape, theft, fraud or other forms of financial exploitation, and certain forms of discrimination, whether on racial or gender grounds.

14.2 In addition, the Mental Capacity Act 2005 specifically states that a Deputy or Attorney is guilty of an offence if s/he ill-treats or wilfully neglects the client.

14.3 If there is the possibility of a criminal offence having occurred, it is important to ensure that the Police are involved immediately, and that the criminal investigation takes precedence in the investigation. It is important to act quickly and if in doubt to contact the Police for advice on whether a crime has been committed.

14.4 Whether to involve the Police during the course of an investigation will be a matter for the Compliance and Regulation manager and Head of Supervision or in urgent situations a member of the executive team, if necessary, in consultation with the OPG Legal Advisor, as it will not always be clear-cut. At the end of an investigation, the Public Guardian (or Head of Supervision in his absence) will make the decision. The OPG's legal advisor must be consulted if witness statements are required.

Public Protection Units

Public Protection Units are specialist units in local police forces that commonly manage and investigate crimes involving adult abuse, child abuse, domestic abuse, sex and dangerous offenders and vulnerable and intimidated witnesses. They are normally staffed with specialist officers trained on interviewing children and vulnerable adults.

15. Records and reporting

15.1 It is essential to keep a written record of *every* discussion, contact, investigation, and decision with regards to suspected or actual abuse. This is equally important whether a decision is made to follow up the suspicion/allegation or to do nothing. If a decision not to take any action is made, then be clear as to why this is. If any further incidence occurs in the future these records will contribute to decisions made at that time.

15.2 All records that record suspected or actual abuse should include within the document:

• The date created.

• The author of the document; and

• The protective marking of the information (e.g., protect, restricted) in bold at the top of the first page (see guidance on '*How to apply protective marking'* on the OPG intranet)

15.3 All records must be captured in relevant recordkeeping systems in a timely fashion, following OPG's Records Management Policy (see intranet).

15.4 All phone discussions with other agencies should be recorded in writing and confirmed by writing to the agency verifying what was discussed.

15.5 Files and CASREC records of clients where there is an active investigation of abuse should be marked to show this is the case, so that anyone dealing with issues relating to that client is aware.

1 Glossary*: Process for action in response to suspected or alleged abuse.*

SUSPICION, REPORT OR EXPRESSION OF CONCERN

All staff - Immediate Action to be taken on the day the suspicion, allegation or report is raised:

• Ensure the safety of the individual. If in immediate danger, contact the relevant emergency services, e.g., police, ambulance.

• If contact is via telephone, record what is being said but avoid asking any leading questions. Obtain details and a contact number of the person reporting the concerns and the vulnerable adult.

• Complete the abuse alert form in Appendix 2. Pass with any supporting documentation to the Compliance and Regulation team to evaluate seriousness and assess any further action.

• If allegation relates to a staff member or visitor, refer to the relevant Head of Division and the Head of Finance and Resources

• Ensure all discussions and decisions are recorded.

Within 24 hours – Compliance and Regulation team

• Consider the urgency and risk to the vulnerable adult and record this assessment

• Consider reporting incident to the Police (Public Protection Unit) if criminal offence appears to have been committed

• Consider referral to Adult Care Social Services or Emergency Duty service

• Consider referral to CSCI/CSIW if alleged abuse relates to care staff (residential or domiciliary)

• Alert Court admin staff to any immediate concerns about pending court applications

• If investigation is deemed necessary, record on database

• If case is subject to Type 1 supervision, liaise with Supervision Casework team

• Record all actions and decisions

On-going action may include.

• Section 58 or Reg 48 investigation and report to PG

• Applications to Court

• Visit

• Participate in Police or Adult Care Social Services Investigation, consider attending strategy meetings

• Liaison with other agencies, e.g., CFO, banks, care homes

• Respond to person raising concerns

• Deputyship moved to close (Type 1) supervision

• Seek HR involvement in any internal investigation and advice on POVA/ISA list

Information to be given when making a referral to external agencies.

• Details of alleged victim (name, contact details, DOB, gender, ethnicity and principal language, any disability, any known communication issues)

• Name and contact details of GP, if known

• Reasons for the concerns, the context for these and how they came to light

• An impression of the seriousness of the situation

• Any concerns about the person's mental capacity

• Whether the person is aware of and has consented to the referral

• Action already taken by the OPG to protect the person

OPG Safeguarding Vulnerable Adults Page Procedures & Guidance

2 Glossary*:* ABUSE ALERT FORM: INTERNAL USE ONLY PROTECT

To be completed following an allegation, suspicion, or report of abuse under the Safeguarding Vulnerable Adults procedures.

To be completed and forwarded on the day of the alert. Form completed by	Contact telephone number
Position	Date
Team	

Part 1: Alleged victim Part 1: Alleged victim

if there is more than one alleged victim, fill in a separate sheet for each alleged victim or provide details in part 5

if there is more than one alleged victim, fill in a separate sheet for each alleged victim or provide details in part 5 First name(s)			
Surname			
Address			
Postcode			
Casrec/Meris ref (if known)		If Deputyship, is the case Type 1 supervision?	YES/NO

To complete the remainder of this form. Attach the correspondence and pass it to the Compliance and Regulation team (Supervision Division)

Part 2: details of organisation or person alerting abuse

Address			
Contact Tel no			
E mail address			
Does the alerted wish to remain anonymous?	**Yes**	**No**	
Does the alerter's identity need protecting?	**Yes**	**No**	**Not known**

What is the relationship of the person/organisation alerting abuse to the alleged victim?

_____

Part 3: alleged perpetrator/s

If there is more than one, fill in a separate sheet for each alleged perpetrator or detail in Part 5

Name not known	
Alleged perpetrator not known	
First name/s	
Surname	
Address/organisation	
Postcode	
Tel no (if known)	

Relationship of alleged perpetrator to alleged victim _____

Are others at risk?

Yes	No	Not known

If yes, please specify _____

_____

If the alleged perpetrator is responsible for others as an employer/employee/carer/volunteer, please state:

Alleged perpetrator's job title/role	
Alleged perpetrator's employer	

Part 4: type of abuse suspected please *tick as many as apply*

Financial/material		Psychological		Institutional	
Neglect		Discriminatory		Sociological	
Physical		Sexual			

Please detail the concerns, continue on separate sheet if needed.

_____

_____

_____

_____

Is the concern about a "one-off" incident or are there ongoing concerns?

Is the concern an allegation or a suspicion or is there actual evidence of abuse (e.g. witnessed behaviour)? _____

What are the alleged victim's circumstances? (E.g. lives alone, lives with alleged perpetrator, lives in care home) ----------

Is the alleged victim aware of the referral?	Yes		No		Not known	

Part 6: Key contacts

Please detail anyone involved with the alleged victim who may be able to assist an investigation, e.g. Adult Care Social Services, G.P., family/carers. Provide contact details where known.

Contact name (1)		Contact name (3)	
Contact details (Tel no, etc)		Contact details (Tel no, etc)	
Relationship to alleged victim		Relationship to alleged victim	
Contact name (2)		Contact name (4)	
Contact details (Tel no, etc.)		Contact details (Tel no, etc.)	
Relationship to alleged victim		Relationship to alleged victim	

Part 7: Immediate action taken to prevent immediate risk *please detail any action taken to prevent immediate risk*

Police (Inc. time/date/crime/log no)	
Ambulance	
Fire	
GP	
Other (please specify)	
Name of manager consulted about immediate action	

PLEASE PASS THIS FORM WITH ANY DOCUMENTARY EVIDENCE TO THE COMPLIANCE AND REGULATION TEAM (SUPERVISION DIVISION)

NB if the allegation is about a member of staff, Visitor or Contractor, the appropriate Head of Division and the Head of Finance and Resources must be notified without delay.

3 Glossary: Information Sharing Protocol

This protocol sets out the legal framework, principles and good practice that apply to information sharing between the OPG and Local Authorities when considering safeguarding issues for vulnerable adults.

Nothing in this framework overrides any legal obligation on the OPG or Local Authorities to share information in specified circumstances, e.g., under the requirements in the Safeguarding Vulnerable Groups Act.

What information may be shared?

Information shared should be on a “need to know” basis, i.e., it should only be information that is directly relevant to the investigation, and the minimum necessary to achieve the objective of protection of vulnerable adults. Care should also be taken to ensure the quality of the information shared, e.g., names, addresses and dates of birth are accurately recorded.

Information about a client, an alleged perpetrator, or others, which may be shared includes:

• Contact details, e.g., names, addresses, telephone numbers, email addresses

• Personal details, e.g., national insurance numbers, dates of birth, family and close contacts, carer’s details.

• Information about someone’s health or welfare, e.g., G.P., details of care/support packages.

• Financial information, e.g., bank details, investments

• Sensitive information, e.g., details of alleged abuse.

When information will be shared

Information will be shared where consent is given to do so in compliance with GDPR 2018.

Information will be shared on a need-to-know basis with appropriate selection of information.

The scenarios that this protocol covers are:

• Where it is practicable to obtain the individual's consent, and consent is given

• Where a decision is taken to apply an exemption under GDPR 2018. e.g., prevention or detection of crime, obtaining legal advice.

• Where it is in the public interest to share the information

• Where the OPG wants to obtain information from a Local Authority about a safeguarding matter

• Where the OPG wants to disclose information to a Local Authority so that they can carry out their own investigation

• Where a Local Authority is carrying out an investigation and asks the OPG to disclose information to it by way of assistance

• Joint investigations by the OPG and Local Authority in regard to a safeguarding matter

• Where the OPG is carrying out its own investigation

For other scenarios not listed above, staff should seek guidance from the Departmental Legal Team to ensure that information is shared within the requirements of the law.

Local authorities and the OPG may not share information that has been provided by their respective organisations with other organisations and individuals unless:

Permission is given by the person about whom the information is held, *or*

There is an overriding justification, legal requirement, or duty to share information without the person's consent.

When the person does not have the capacity to consent to information sharing

If an adult does not have capacity to make a decision about consenting to information sharing, others can take that decision on their behalf. Capacity to be able to give consent can be assessed by considering:

• does the person have a general understanding of what decision they need to make and why they need to make it?

• has the person got the ability to understand and retain the information relevant to the decision?

• will they be able to understand the reasonably foreseeable consequences of deciding one way or another?

• do they have the ability to communicate (by any means) the decision they have come to?

Where a person is not the legal representative but acts as a "carer" to a person not capable of giving consent, it should be considered whether they are acting on their behalf and in the individual's best interests.

Why information may be shared.

The objective of sharing information will be to achieve where possible:

• The safeguarding of vulnerable adults

• Appropriate sharing of information between agencies for the benefit of safeguarding the vulnerable adult

• Prompt identification of abuse

• Prevention of abuse, or prevention of further abuse

• Safeguarding other vulnerable adults

• Dealing with a perpetrator of abuse

Personal and sensitive information will be shared in compliance with the requirements of the GDPR 2018, i.e. where there is a legal obligation, it is to do with the administration of justice, it is “in the vital interest of the data subject” (in the best interest of a vulnerable adult) or “in the public interest” (e.g. where others in the same care setting may be at risk).

Benefits of sharing information (outcomes)

A number of agencies may be involved in different aspects of the care and support of a vulnerable adult. The benefits of sharing information in the above circumstances are:

• Agencies can pool information and expertise to resolve problems

• Intelligence is shared, and a full picture obtained that will initiate appropriate action

• To enable investigations

• To assess the risk to the vulnerable adult and others

• To put in place protective measures

Data handling of client information

Information may be shared in the context of an investigation into abuse without the individual’s knowledge or consent. This may be because the vulnerable adult may be unable to give informed consent, or because obtaining consent or notifying someone that information will be shared may prejudice the outcome of an investigation. The consent of the subject of the information will be sought wherever possible and where it will not undermine the purpose of the disclosure.

Individuals have a right of access to information recorded about them. The OPG and individual Local Authorities publish information about how individuals may access their records and will ensure that shared information is covered by their records management and Information Security policies and practice.

It is the responsibility of the OPG and individual Local Authorities to ensure that there is no unauthorised access, loss, misuse, modification, or disclosure of someone’s personal or sensitive information.

Legal framework

Data protection Act 2018 and The Data Protection (Processing of Sensitive Personal Data) Order 2000.

The conditions for disclosure that are relevant to this document are in Schedules 2 and 3 of the Data Protection Act 2018 and include conditions 3 (legal obligation) and 5 (e.g., administration of justice) of Schedule 2, as well as condition 4 (vital interests of the data subject). Schedule 3 conditions 6 and 7 are also relevant to the processing of sensitive personal information and its disclosure.

The Data Protection Act permits the sharing of personal information when it is:

i. in the vital interest of the data subject, or

ii. in the public interest

Mental Capacity Act 2005

Section 58(2) of the Mental Capacity Act 2005 provides for the Public Guardian's duties to supervise Deputies and investigate concerns about the way a Deputy or Attorney is exercising their powers to be discharged "in co-operation with any other person who has functions in relation to the care or treatment of P" (the person lacking capacity).

Section 58(5) of the Mental Capacity Act 2005 gives the Public Guardian authority, in the course of carrying out his duties, to examine and take copies of any health record, any record of, or held by, a Local Authority and complied in connection with a social services function, and any record held by a person registered under Part 2 of the Care Standards Act 2004 (c.14), so far as the record relates to P.

This authority does not extend to records relating to a Deputy or Attorney.

Information Security

Ensuring security of information

The OPG aims to ensure that there will be no unauthorised access to, loss, misuse, modification or disclosure of its client's information. It respects a client's right to privacy and understands that information may be imparted to in a relationship of confidence. It will ensure that disclosure is proportionate to the matter under investigation.

The following standards will be applied when exchanging information with Local Authorities.

Telephone calls

If the Local Authority requests information about a client, the OPG will verify who the caller is before releasing any information. Verification may be carried out by calling back the person on a number recorded in the OPG's case file or asking for the query to be e- mailed. Once received, the e-mail will be checked that it has come from a Local Authority and the contact can be called back.

Use of e-mail

External e-mails sent between Local Authorities and the OPG are not encrypted in any way; nor are they transmitted over a secure medium. To avoid unauthorised disclosure of personal information, the OPG applies the following standards to e-mail correspondence:

The OPG will not send any personal information about a client or deputy, e.g., information about finances or personal circumstances via e mail. E mails received by the OPG that contain personal information will be acknowledged and replied to by letter within published correspondence targets. If urgent, a letter may be sent as an attachment to an e-mail, in which case it will be password protected and the password sent in a separate e mail. Staff will take care to confirm e mail addresses and will keep personal information to a minimum.

E-mail communications can be used for non-case specific enquires, to send information about OPG services, to send electronic forms and templates, and to acknowledge receipts of letters, etc.

Paper documents and records

The OPG applies a system of protectively marking personal information and applying handling controls according to the sensitivity of the information and risk of unauthorised disclosure. Documents containing personal information can be sent to Local Authorities by ordinary letter post. Depending on the level of risk, documents may be double enveloped to ensure secure delivery. The outer envelope will not bear any markings or notations to indicate that the contents are protectively marked. Envelopes will be marked with a return address in the event of non-delivery.

Information security breaches

Any breach of procedure and or loss of information must be reported immediately by the member of staff who has discovered the breach to their Line Manager who will inform their Head of Department. Reporting of information security breaches within the OPG should follow the OPG Post-Incident Response Plan, a copy of which can be found on the OPG intranet. Loss of OPG information held outside of the OPG must be reported immediately to the OPG Records Manager.

4 Glossary

Abuse

Abuse is a violation of an individual's human and civil rights by another person or persons. Abuse may consist of a single act or repeated acts. It may be physical, verbal or psychological, it may be an act of neglect or an omission to act, or it may occur when a vulnerable person is persuaded to enter into a financial or sexual transaction to which he is she has not consented or cannot consent. Abuse can occur in any relationship and may result in significant harm to, or exploitation of, the person subjected to it.

Appointee

Someone appointed under Social Security regulations to claim and collect social security benefits on behalf of a person who lacks capacity to manage their own benefits.

Attorney

Someone appointed under either a Lasting Power of Attorney (LPA) or an Enduring Power of Attorney (LPA), who has the legal right to make decisions within the scope of their authority on behalf of the person (the donor) who made the power of attorney. Also known as a donee.

Care home

A home registered with the Commission for Social Care Inspection, or Care and Social Services Inspectorate in Wales that provides accommodation with personal care. A care home with nursing provides nursing and personal care.

Commission for Social Care Inspection (CSCI)

The single, independent inspectorate for social care (all care providers) services in England.

Capacity

The ability to make a decision about a particular matter at the time the decision needs to be made. The legal definition of a person who lacks capacity is set out in section 2 of the Mental Capacity Act 2005.

Care and Social Services Inspectorate in Wales (CSSIW)

The single, independent inspectorate for social care (all care providers) services in Wales.

Care package

Services designed to meet an individual's assessed needs as part of the care plan arising from their assessment. Consists of one or more services, which may be residential and/or community based. Where necessary this covers both NHS and social care.

Care plans

Written agreements setting out how care will be provided within the resources available for people with complex needs.

Care Quality Commission

From April 2009, the Care Quality Commission will have responsibility for regulating and improving the quality of health and social care in England and will look after the interests of people detained under the Mental Health Act. It takes over the work of the Commission for Social Care Inspection, the Healthcare Commission, and the Mental Health Act Commission.

Carer

Person who provides a substantial amount of care on a regular basis and is not employed to do so by an agency or organisation. Carers are usually friends or relatives looking after someone at home who is elderly, ill or disabled.

Care worker

Paid workers that support people with everyday tasks who may be elderly, ill, have physical or learning disabilities, or emotional or social problems.

Continuing care

The criteria for assessing and providing health and social care over an extended time as the result of disability, accident, or illness, in order to meet both physical and mental health needs. Continuing care can be provided in a range of settings, including hospital, care home or hospice and the individual's own home. Continuing care aims to provide the right long-term support, to promote independence, prevent deterioration and maximise a person's health and quality of life.

Court of Protection

The specialist Court for all issues relating to people who lack capacity to make specific decisions.

Court of Protection Visitor

Someone who is appointed to report to the Court of Protection or Public Guardian on how attorneys or deputies are carrying out their duties.

Criminal Records Bureau (CRB)

An executive agency of the Home Office which provides access to criminal records information. Organisations in the public, private and voluntary sectors can ask the CRB to check candidates for jobs to see if they have any criminal records which would make them unsuitable for certain work especially that involves children or vulnerable adults.

GDPR 2018

A law controlling the handling of, and access to, personal information, such as medical records, files held by public bodies and financial information held by credit reference agencies.

Day Centre

Facility, run by social services, health or a voluntary organisation, that provides care, stimulation and activities for people who need support during the day and is thus also a valuable source of respite for carers.

Declaration

A kind of order made by the Court of Protection, e.g., whether a person has or lacks capacity to make a particular decision or declaring that a particular act would or would not be lawful.

Dementia

Term used for different illnesses that affect the brain and diminish the ability to do everyday tasks. 'Dementia' should be used to describe symptoms, not the condition itself. Symptoms include loss of memory; difficulty in understanding people and finding the right words; difficulty in completing simple tasks and solving minor problems; mood changes and emotional upsets.

Deputy

Someone appointed by the Court of Protection with ongoing legal authority as prescribed by the Court to make decisions on behalf of someone who lacks capacity to make particular decisions. A Deputy may be appointed to make decisions in relation to property and affairs (financial) or welfare (including healthcare), or both. A Deputy may be a professional, e.g., solicitors, local authorities, or lay, e.g., family members, friends of the person lacking capacity.

Domiciliary care

Homecare that helps people cope with disability or illness and allows them to maintain independence.

Donee

Someone appointed by a Donor to make decisions under a Lasting Power or Enduring Power of Attorney.

Donor

A person who makes a Lasting Power of Attorney or Enduring Power of Attorney.

Enduring Power of Attorney (EPA)

A power of attorney created under the Enduring Powers of Attorney Act 1985 appointing an attorney to deal with the donor's property and financial affairs. The Mental Capacity Act 2005 replaced the EPA Act 1985 but existing EPAs continue to operate under Schedule 4 of the Act.

Health

State of complete physical, mental and social well-being – not merely the absence of disease and infirmity

Health Care Commission

The independent watchdog for healthcare (NHS and private) in England.

Health Care Inspectorate Wales (HIW)

A department of the National Assembly for Wales with responsibility for inspecting and investigating the provision of health care by and for Welsh NHS bodies.

Independent Mental Capacity Advocate (IMCA)

Someone who provides support and representation for a person who lacks capacity to make specific decisions, where the person has no-one else to support them.

Independent Safeguarding Authority (ISA)

The Independent Safeguarding Authority's role is to help prevent unsuitable people from working with children and vulnerable adults. From October 2009, employers will be required to ensure that any staff they have working with children or vulnerable adults are checked by the ISA and have gone through the registration process with the Criminal Records Bureau.

Key Worker

Person responsible for co-ordinating the care plan of an individual receiving social care, for monitoring their progress, and for staying in regular contact with the agencies and individuals involved.

Lasting Power of Attorney (LPA)

A power of attorney created under the Mental Capacity Act appointing an attorney or attorneys to make decisions about the donor's personal welfare (including healthcare) and/or deal with the donor's property and affairs.

Learning disabilities

Disabilities that reduce a person's ability to understand new or complex information, learn new skills and cope independently.

Local Authority

Elected council responsible for providing public services such as education, housing and social services within a particular area. Most urban areas, including London, have unitary authorities i.e. one council provides all local government services

Long term conditions

Conditions, such as diabetes, asthma and arthritis that cannot currently be cured, but whose progress can be managed and influenced by medication and other therapies.

NHS Trusts

Hospitals, community health services, mental health services and ambulance services that are managed by their own boards of directors. NHS trusts provide services on the requirements of patients as represented by primary care trusts.

Nursing Home

Care home that provides nursing care (with, generally, at least one registered nurse on duty). Under the Care Standards Act 2000, which came into effect in April 2002, nursing homes were renamed 'care homes with nursing'.

Office of the Public Guardian (OPG)

An agency of the Ministry of Justice. The Public Guardian is an officer established under section 57 of the Mental Capacity Act 2005. The OPG supports the Public Guardian to support and promote decision-making for those who lack capacity or wish to plan for their future. It registers powers of attorney, and supervises deputies appointed by the Court of Protection to make decisions on behalf of someone who lacks capacity. It also provides administrative support to the Court of Protection. The OPG replaced the Public Guardianship Office (PGO).

Primary care

The collective term for all services which are people's first point of contact with the NHS, egg GPs, dentists.

Primary care trusts (PCTs)

NHS bodies with responsibility for delivering health care services and health improvements to their local areas. Commissions primary care services within a particular area and is also responsible for providing local community health services.

Protection of vulnerable adults (POVA)

Public body initiative set up to specifically address the abuse of vulnerable adults. The POVA list is a register of individuals who have abused, neglected, or otherwise harmed vulnerable adults in their care or placed vulnerable adults at risk of harm. A way of preventing the employment of people who should not be appointed to positions of trust e.g., Carers.

Public Protection Units

Public Protection Units are specialist units in local police forces that commonly manage and investigate crimes involving adult abuse, child abuse, domestic abuse, sex and dangerous offenders and vulnerable and intimidated witnesses. They are normally staffed with specialist officers trained on interviewing children and vulnerable adults.

Social Services Department (Adult Care Social Services)

Department of local authority providing needs assessments to determine individuals' eligibility for assistance and ascertain how support can be given to meet eligible needs. Also provides and purchases a range of residential, day and domiciliary care packages to support people in need.

Vulnerable adult

The definition of vulnerable adult that applies to Adult Care Social Services is "a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation."

The OPG's policy on safeguarding vulnerable adults applies to anyone who has a Deputy appointed by the Court of Protection or is the donor of a registered EPA or LPA or is someone for whom the Court of Protection has authorised a person to carry out a transaction on their behalf under s16 (2) (d) of the Mental Capacity Act (single orders).

PREVENT

Prevent forms one part of the Government's overall counter terrorism strategy, 'CONTEST', which is led by the Home Office. CONTEST is primarily organised around four key principles or work streams, each with a specific objective:

- PREVENT To stop individuals becoming terrorists or supporting terrorism.
- PURSUE To disrupt or stop terrorist attacks occurring.
- PROTECT To strengthen our borders, infrastructure, buildings, and public spaces from a terrorist attack.

- PREPARE To reduce the impact of an attack if an act of terrorism occurs.

Prevent is aimed at front line staff and is designed to help make staff aware of their role in preventing. vulnerable people being exploited for terrorist purposes.
The Counter Terrorism and Security Act (2015) places a duty on a range of organisations to have due. regard to the need to prevent people of all ages being drawn into terrorism.
The Prevent strategy recognises that NHS staff may come into contact with individuals (both children and adults) who are vulnerable to radicalisation. Radicalisation is usually a process, not a one-off event, and during that process it is possible to intervene to safeguard the vulnerable individual before any harm has occurred or crime has been committed. Staff must have an awareness of the risk of radicalisation, identify those individuals who may be vulnerable and intervene to prevent them from supporting. terrorism or becoming terrorists themselves.
If a staff member has concerns that a child or adult may have been radicalised or is at risk of radicalisation, staff must be aware of their responsibilities under this policy to report their concerns and complete a Prevent referral to the Local Authority.
All concerns relating to Prevent must be escalated as a matter of urgency to the Corporate Safeguarding Team.
The Prevent referral process can be described in three stages: notice, check and share.

Notice: Staff must be aware of an individual's vulnerability to radicalisation, changes in behaviour, ideology and other forms of extremism.
Check out your concerns with the individual where possible, and were safe, with your line manager, colleagues and Multi-Disciplinary Clinical meetings. Checking out your concerns with the Southern Health Safeguarding Team will help to ensure a proportionate response to the concerns.
Share your concerns with partner agencies, and as far as possible be open and honest with the individual about the duty to share your concerns.
On raising a concern or completing a Prevent referral form, a Ulysses Incident Report must be completed.

Part 7 Current Staff & Positions

Current Staff

Name	Position	Name	Position
Bronwen Cook	MD	Dave Harding	CITB Tutor
George Walton	Manager/ Invigilator/ IQA / H & S Manager /EQA	Aidan Earp	Peripatetic Instructor
James Cook	Accounts-MD Invigilator/IQA	Russ Hudson	Peripatetic Instructor
David Owen	NVQ Co-ordinator	Ewan Marrows	Peripatetic Instructor
Lindsay Weaver	Administrator	James Limpkin	Peripatetic Instructor
Mike Halliday	Instructor/Assessor/IV	Oliver Keates	Peripatetic Instructor
Chris Sharp	Instructor		
Maureen Pringle	Instructor/Assessor/IV		
Barry Richardson	Instructor/Assessor		
Jason Lightfoot	Instructor/Assessor/IV		
Rick Culley	Instructor		
Janet O'Keeffe	Admin/Invigilator/IQA		
Jonathan Edmonds	Instructor		

Keith Cook Training Limited			Site-Specific Risk Assessment
Course title			
Accrediting Body		Date	
Venue			

Please check your details, and sign to indicate your presence on this course and your understanding of the risk assessment on the reverse of this form.

I understand the risk assessments that have been carried out for the event that I am attending and the control measures that must be implemented. I have also received information regarding action in case of fire, medical emergency and accident reporting and recording.

Name	Emergency Contact No	Signature

Certificates Printed		Initials and Date	
Certificates issued		Initials and Date	

Training Course or Assessment		Date of course or Assessment	
Client Company		Number of trainees or candidates	
Location including Postcode		Client Company emergency contact and phone no.	
Meeting point for emergency vehicles		OS Grid reference	
Nearest Hospital with A&E		Nearest Landline Phone location	
Landowner contact address		Landowner phone. Landline & Mobile	
Instructor's Emergency Contact Details		Instructor's Mobile No	
Generic Risk assessment title			
Relevant Tasks			
Additional hazards not covered by generic risk assessment		Additional control methods required to reduce risks to acceptable level.	
Risk assessment completed by: (signature)			
Name		Date	
Control measures implemented by (signature)			
Name		Date	

FIRE RISK ASSESSMENT

For
Keith Cook Training Limited

This document suggests information that should be contained in a fire risk assessment record. It may serve as a record of the significant findings of a fire risk assessment. Further guidance can be found in a booklet called "Fire Safety - An Employer's Guide" published by H.M. Stationery Office ref: ISBN 0-11-341229-0.

1. PREMISES DETAILS

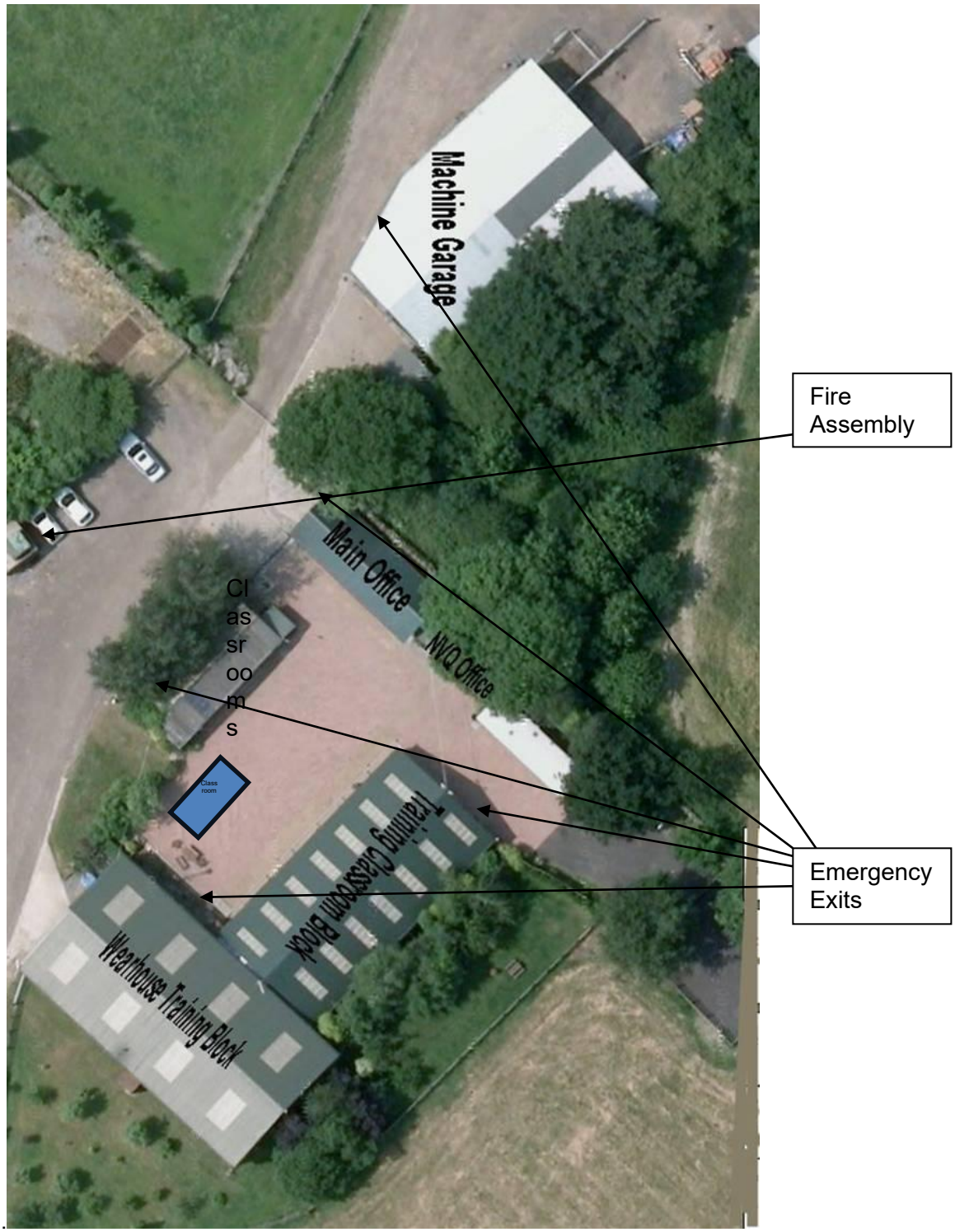
PREMISES ADDRESS	Springfield Farm Charley Road Oaks in Charnwood Leicestershire LE12 9YB
OCCUPIER	Keith Cook Training Limited
OWNER	Bronwen Cook James Cook

RESPONSIBLE PERSON	George Walton
USE & MAXIMUM NUMBER OF PERSONS PRESENT	Training Up to 12 staff and up to 50 trainees/visitors
HOURS PREMISES ARE IN USE	8.30am to 5.30pm Monday to Friday
CONSTRUCTION	Main Office – Wood with metal corrugated roof Warehouse Training Block - Brick with metal corrugated roof Classroom Training Block - Wood with metal corrugated roof
DIMENSIONS	
No. OF FLOORS IN PREMISES	1
No. OF FLOORS IN BUILDING	1
DETAILS OF OTHER PREMISES IF PART OF MULTI-OCCUPIED BUILDING	None
NAME OF ASSESSOR INCLUDING CONTACT DETAILS	Gerry Bungart Fire Proof Ltd Unit 4 Matrix House 18 Constitution Hill Leicester LE1 1PL Tel 0116 248 9555 Mob 0771 415 2875
TRAINING & EXPERIENCE OR KNOWLEDGE OR OTHER	ISO 9001

QUALITIES OF ASSESSOR	BAFE approved and registered technicians Work carried out is in strict accordance with BS53006
DATE ASSESSMENT CARRIED OUT	03rd January 2024
REVIEW DATE	06th January 2025

2. PREMISES PLAN

PREMISES PLAN DETAILING MEANS OF ESCAPE & OTHER PREVENTITIVE & PROTECTIVE MEASURES.



3. HAZARDS

SOURCES OF IGNITION INCLUDING ACTION TAKEN TO REDUCE THE RISK:	
HAZARDS IDENTIFIED	2 x External Refuelling Tanks
EXISTING CONTROL MEASURES	Purposefully constructed tanks with a COSHH assessment completed
ACTION REQUIRED	None

SOURCES OF FUEL INCLUDING ACTION TAKEN TO REDUCE THE RISK:	
HAZARDS IDENTIFIED	As Above
EXISTING CONTROL MEASURES	-
ACTION REQUIRED	None

DETAILS OF ANY HAZARDOUS SUBSTANCES PRESENT:	
HAZARDS IDENTIFIED	None
EXISTING CONTROL MEASURES	-
ACTION REQUIRED	-

HAZARDS FROM WORK PROCESSES - DETAILS INCLUDING ACTION TAKEN TO REDUCE THE RISK:	
HAZARDS IDENTIFIED	Electric charger points for Forklift Trucks
EXISTING CONTROL MEASURES	Powder extinguishers in place with restricted area chained off whilst charging.
ACTION REQUIRED	None

STRUCTURAL HAZARDS:	
HAZARDS IDENTIFIED	Wood construction
EXISTING CONTROL MEASURES	Smoke detectors in place a new fire point system is now in place and fire drills are carried out. Smoke detectors and fire points are visually checked weekly, the fire extinguishers are checked annually
ACTION REQUIRED	None

4. HISTORY

HISTORY OF ANY PREVIOUS FIRES AFFECTING THE PREMISES:	
DETAILS	No
ACTION REQUIRED	None

5. MITIGATING THE EFFECTS OF FIRE

MEANS OF FIGHTING FIRE:	
DETAILS	8 x AFF Foam Extinguishers 5 x CO2 Extinguishers 1 x Powder Extinguishers 1 x Fire Blanket
MATTERS OF CONCERN	None
ACTION REQUIRED	None

MEANS FOR RESTRICTING FIRE SPREAD:	
HAZARDS IDENTIFIED	Self-closing internal doors not installed except for main entrance
EXISTING CONTROL MEASURES	Fire retardant doors
ACTION REQUIRED	Review internal door system.

MEANS OF SEGREGATING AREAS OF HIGHER FIRE RISK:	
HAZARDS IDENTIFIED	None
EXISTING CONTROL MEASURES	-
ACTION REQUIRED	-

6. FIRE DEVELOPMENT

CONSIDERING THE INFORMATION CONTAINED IN SECTION 1 - 5 DESCRIBE THE MOST LIKELY WORSE CASE SCENARIO FIRE SITUATION TO BE ENCOUNTERED.
To include details of estimated fire development and heat and smoke generation. Classroom and office complexes are constructed in wood, which is a high-risk material, however every means of restriction of fire outbreaks have been considered. A fire alarm system has been installing and is now operational and fire drills have been run. This system is also battery backed up so that it will continuously ring even if power is cut. KCT Ltd also have a smoke detector in place throughout the whole location. A Fire Screamer has also been installed.
ACTION REQUIRED:
Continued monitoring and fire drills to be completed.

7. OCCUPANTS

OCCUPANT CHARACTERISTICS:	
DETAILS OF OCCUPANTS	H & S Training Instructors & Assessors Admin Staff Trainees Visitors
DETAILS OF ANY PERSONS CONSIDERED TO BE PARTICULARY AT RISK E.G LONE WORKERS, VISITORS,PEOPLE WITH SPECIAL NEEDS, PEOPLE WHO MAY BE ASLEEP	None
ACTION REQUIRED	None

8. RAISING THE ALARM

MEANS OF DETECTING & GIVING WARNING OF FIRE:	
DETAILS	Fire Alarm System Smoke Detectors Fire Screamer Emergency Lighting Installed in January 2024
MATTERS OF CONCERN	None
ACTION REQUIRED	Weekly checks of Smoke detectors and Fire points

9. ESCAPE ROUTES

ESCAPE ROUTES AND EXITS AVAILABLE FOR OCCUPANTS:	
EXISTING PROVISION	All adequate
MATTERS OF CONCERN	None
ACTION REQUIRED	None

MEANS FOR ENSURING ESCAPE ROUTES CAN BE SAFELY USED DURING EVACUATION:	
EXISTING PROVISION	Weekly walk through site checks
MATTERS OF CONCERN	None
ACTION REQUIRED	None

10. EVACUATION PROCEDURES

EMERGENCY ACTION PLAN:	
EXISTING PROCEDURES	Fire Exits posted, also information on inductions to courses within the risk assessment.
MATTERS OF CONCERN	None
ACTION REQUIRED	None

11. FIRE SAFETY MANAGEMENT

FIRE SAFETY POLICY STATEMENT:	
DETAILS	Within these policies and procedures
MATTERS OF CONCERN	None
ACTION REQUIRED	None

FIRE SAFETY MANAGEMENT SYSTEM IN PLACE:	
DETAILS	George Walton – Manager, took charge of this position in 2008
MATTERS OF CONCERN	None
ACTION REQUIRED	None

PROCEDURES IN PLACE TO MONITOR AND REVIEW FIRE SAFETY PROCEDURES IN THE PREMISES:	
DETAILS	Annual extinguisher checks will now be by Fire Proof Ltd due in Jan annually. Weekly checks (visual) of all fire point/escapes etc
MATTERS OF CONCERN	None
ACTION REQUIRED	None

12. MANTENANCE OF EQUIPMENT

MAINTENANCE PROGRAMME FOR PREVENTITIVE & PROTECTIVE MEASURES:	
DETAILS	Annual inspections completed by Fire Proof Ltd certificate displayed in main office
MATTERS OF CONCERN	None
ACTION REQUIRED	None

13. TRAINING

FIRE SAFETY TRAINING PROVIDED FOR RELEVANT PERSONS:	
DETAILS	None
MATTERS OF CONCERN	None
ACTION REQUIRED	Training is now completed refer to action plan, refresher training to be booked during December 2025

14. RECORDS

RECORDS OF MAINTENANCE & TRAINING:	
DETAILS	Report book for fire alarms and smoke detectors are in place
MATTERS OF CONCERN	None
ACTION REQUIRED	Maintain weekly checks

15. CO-OPERATION & CO-ORDINATION

PROCEDURES IN PLACE TO ENSURE CO-OPERATION AND CO-ORDINATION BETWEEN OCCUPIERS OF RELEVANT PREMISES:	
DETAILS	None
MATTERS OF CONCERN	None
ACTION REQUIRED	None

CONSULTATION CARRIED OUT WITH INTERESTED PARTIES DURING RISK ASSESSMENT PROCESS. E.G. EMPLOYEES/SAFETY REPRESENTATIVES:	
DETAILS	Fire Proof Ltd & George Walton
MATTERS OF CONCERN	None
ACTION REQUIRED	None

PROCEDURES IN PLACE FOR ANY NECESSARY CONTACT WITH EXTERNAL EMERGENCY SERVICES, PARTICULARLY AS REGARDS FIRE-FIGHTING, RESCUE WORK, FIRST-AID AND EMERGENCY MEDICAL CARE:	
DETAILS	Telephone system for calls to the emergency services also all staff are emergency first aid trained
MATTERS OF CONCERN	None
ACTION REQUIRED	None

16. COMPANY VEHICLES

COMPANY VEHICLES:	
DETAILS	Company vehicles will not be fitted with any extinguishers as per Company Policies and Procedures, in the case of a fire breaking out in a vehicle all staff must leave the vehicle and NOT attempt to extinguish the fire; they should retreat to a safe distance and call the emergency services.
MATTERS OF CONCERN	None
ACTION REQUIRED	None

17. CONCLUSIONS

CONCLUSION:
KCT Ltd have a training facility used by companies for industrial and construction for plant and lift truck training for 5 national accrediting/awarding bodies. **All fire appliances were brand new in December 2013, an annual inspection is in place and will be conducted by Fire Proof Ltd in January annually, and the letter of confirmation is displayed in the main office.** **Fire extinguisher training was started with Leicester College for December 2009, where all staff attended and completed the course; refreshers will be completed in December every three years.** **The main training classroom area and offices are constructed in wood and all necessary fire precautions have now been addressed.** **Since the introduction of the new fire extinguishers in 2013 replacements have been made during this time.** **New installation of Heat Source pumps for better heating supplies all units are individually installed and isolated.**
ACTION REQUIRED:
Review January 2025

KEITH COOK TRAINING LIMITED'S REMEDIAL ACTION PLAN

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
Fire Alarm System	Install an alarm system	19/12/2008	2/4/2009	George Walton
Fire Extinguishers Training Required	Training Booked for December 2009	31/12/2009	18/12/2009	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2010	31/12/2010	19/1/2010	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2011	31/1/2011	19/1/2011	George Walton
Fire Extinguishers Training Required	To be booked during May 2012	31/12/2012	31/12/2012	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2012	31/01/2013	19/01/2013	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2013	31/01/2014	22/01/2014	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2013	31/01/2015	06/01/2015	George Walton
Fire Extinguishers Training Required	To be booked during December 2015 book with Dave Harding	31/12/2015	23/12/2015	George Walton

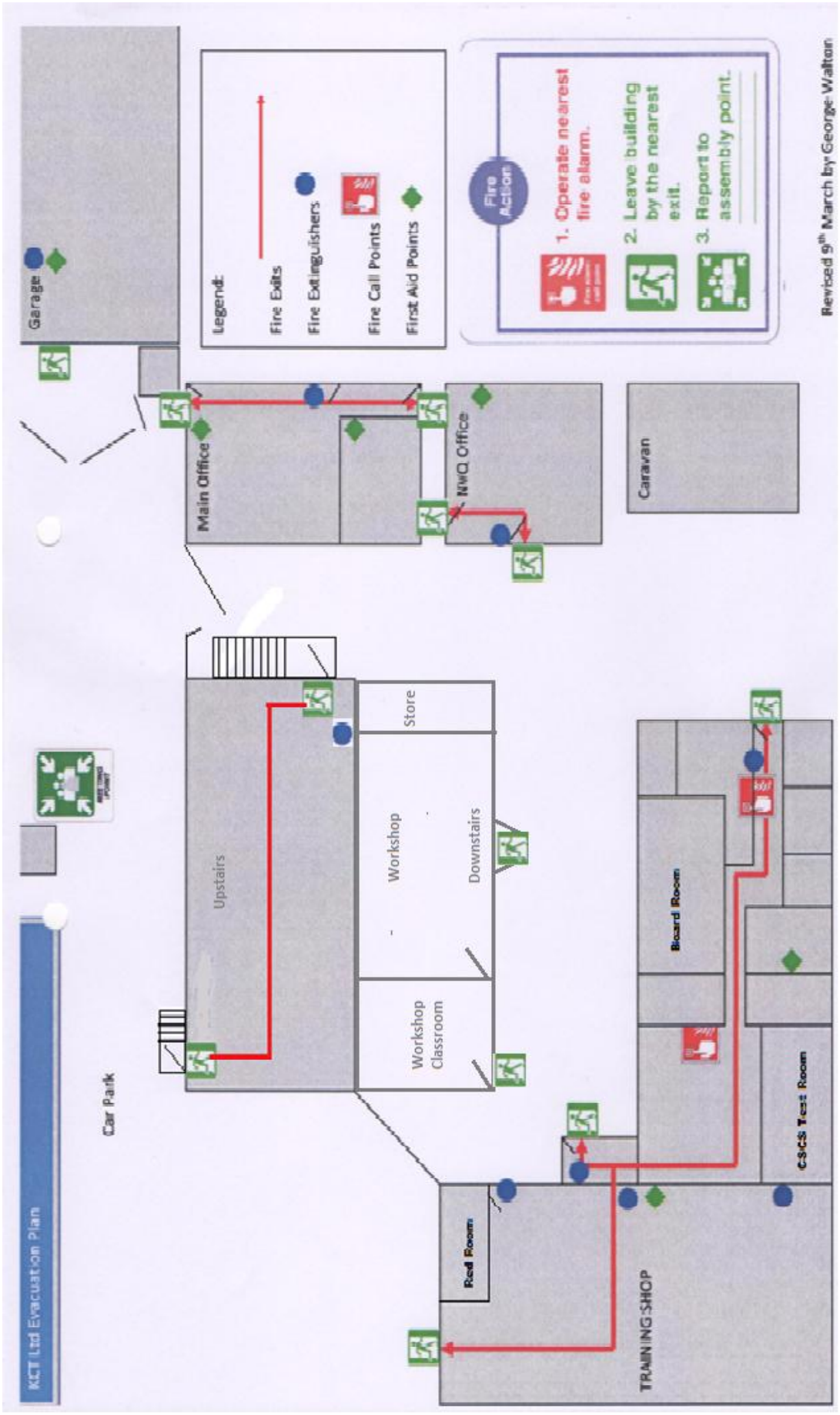
DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
Annual Fire Extinguisher checks	Annual check booked for January 2017	31/01/2017	31/01/2017	George Walton
Annual Fire Extinguisher checks	Annual check booked for January yearly. 5 new CO2 Extinguishers installed. 1 new Foam Extinguisher installed	31/01/2018	12/01/2018	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2019	12/01/2019	12/1/2019	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2020 1 Extinguisher re gassed	12/01/2020	13/01/2020	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2021	13/01/2021	13/01/2021	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2021	13/01/2021	11/01/2021	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2022	13/01/2022	27/01/2022	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2023	13/01/2023	13/01/2023	George Walton
Fire Extinguishers Training Required	To be booked during December 2022 book with Dave Harding	23/12/2022	23/12/2022	George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2024	13/01/2023	17/01/2023	George Walton

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
Fire Extinguishers Training Required	To be booked during December 2025 book with Rick Culley	23/12/2025		George Walton
Annual Fire Extinguisher checks	Annual check booked for January 2024	11/01/2024	11/01/2024	George Walton

OTHER RELEVANT INFORMATION

Fire drills have now been completed, KCT Ltd also had a power cut which also set these alarms off proving that the battery system works.

KCTL Evacuation Map



Part 8 Safeguarding Adults Policy Statement Including Prevent

POLICIES ON SLAVERY AND HUMAN TRAFFICKING

We are committed to ensuring that there is no modern slavery or human trafficking in our supply chains or in any part of our business.

Our Anti-Slavery and Human Trafficking Policy reflects our commitment to acting ethically and with integrity in all our business relationships and to implementing and enforcing effective systems and controls to ensure slavery and human trafficking is not taking place anywhere in our business and in our supply chains. Accompanying this is our Whistleblowing Policy which provides a system for our employees to escalate slavery and human trafficking issues and breaches of our policies.

DUE DILIGENCE PROCESSES FOR SLAVERY AND HUMAN TRAFFICKING

As part of our initiative to identify, monitor and mitigate against industry risk, business transaction risk and risk in the countries in which we operate, we nominate senior representatives of the business units and functions, who in turn report to the Risk and Compliance Manager.

We have in place policies and systems across our business our supply chains to:-

• Identify inappropriate employment practices.

• Identify, assess and monitor other potential risk areas.

• Mitigate the risk of slavery and human trafficking occurring.

• Protect whistle-blowers; and

• Investigate reports of Modern Slavery.

SUPPLIER ADHERENCE TO OUR VALUES AND ETHICS

We have zero tolerance to slavery and human trafficking. To ensure all those in our supply chain and contractors comply with our values we operate in line with principles of responsible sourcing, including paying employees at the prevailing minimum wage applicable within their relevant country of operations.

TRAINING

To ensure a high level of understanding of the risks of modern slavery and human trafficking in our business, in our supply chains, we provide relevant in-house training.

Conduct we also require our business partners to provide regular and relevant training to their staff and suppliers and providers.

COVID-19

We understand that some workers may be more vulnerable to modern slavery during the coronavirus pandemic. The Group adopted government guidelines for Covid-19 secure workplaces and paying statutory sick pay in order to prevent the spread of coronavirus. Our employees have been and continue to have access to our grievance procedures.

NEXT STEPS

• Raise awareness of the Anti-Slavery and Human Trafficking Policy with our employees

• Additional training for employees as necessary.

• Integrate any learnings from Covid-19 into our future strategy.

STATEMENT

This statement is made pursuant to section 54(1) of the Modern Slavery Act 2015

and constitutes our Group's slavery and human trafficking statement for the financial

year ending 31st December 2019 and was approved by the Board of Directors of Countrywide plc on 28 January 2021.

This policy will enable KEITH COOK TRAINING LIMITED to demonstrate its commitment to keeping safe the vulnerable adults with whom it works alongside. KEITH COOK TRAINING LIMITED acknowledges its duty to act appropriately to any allegations, reports or suspicions of abuse.

It is important to have the policy and procedures in place so that staff, volunteers, service users and carers, and management committee can work to prevent abuse and know what to do in the event of abuse.

- The Policy Statement and Procedures have been drawn up in order to enable Keith Cook Training Limited to:
- Promote good practice and work in a way that can prevent harm, abuse and coercion occurring.
- To ensure that any allegations of abuse or suspicions are dealt with appropriately and the person experiencing abuse is supported.
- And to stop that abuse occurring.
-
- The Policy and Procedures relate to the safeguarding of vulnerable adults. Vulnerable adults are defined as:
- People aged 18 or over.
- Who are receiving or may need community care services because of learning, physical or mental disability, age, or illness?
- Who are or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation.
    - (No Secrets, Department of Health, 2000)
- The policy applies to all staff, including senior managers, management committee members, trustees, paid staff, volunteers, sessional workers, agency staff, students and anyone working on behalf of Keith Cook Training Limited
- It is acknowledged that significant numbers of vulnerable adults are abused, and it is important that Keith Cook Training Limited has a Safeguarding Adults Policy, a set of procedures to follow and puts in place preventative measures to try and reduce those numbers.
- In order to implement the policy, the Keith Cook Training Limited will work:

- to promote the freedom and dignity of the person who has or is experiencing abuse.
- to promote the rights of all people to live free from abuse and coercion.
- to ensure the safety and wellbeing of people who do not have the capacity to decide how they want to respond to abuse that they are experiencing.
- to manage services in a way which promotes safety and prevents abuse.
- recruit staff and volunteers safely, ensuring all necessary checks are made.
- provide effective management for staff and volunteers through supervision, support and training.

Keith Cook Training Limited:

- will ensure that all management committee members, trustees, staff, volunteers, service users, and carers/families are familiar with this policy and procedures.
- will work with other agencies within the framework of the Policy and Procedures, issued under No Secrets guidance (Department of Health, 2000)
- will act within its confidentiality policy and will usually gain permission from service users before sharing information about them with another agency.
- will pass information to Adult and Culture Services when more than one person is at risk. For example: if the concern relates to a worker, volunteer or organisation who provides a service to vulnerable adults or children.
- will inform service users that where a person is in danger, a child is at risk, or a crime has been committed then a decision may be taken to pass information to another agency without the service user's consent.
- will make a referral to the Adult Social Care Direct team as appropriate.
- will endeavour to keep up to date with national developments relating to preventing abuse and welfare of adults.
- will ensure that the Designated Named Person understands his/her responsibility to refer incidents of adult abuse to the relevant statutory agencies (Police/Adult and Culture Services Directorate)

The Designated Named Person for Safeguarding Adults in Keith Cook Training Limited is George Walton/Michael Halliday 01509 600330

- They should be contacted for support and advice on implementing this policy and procedures.
-

These are kept in the main office at KCT Ltd

Prevention and awareness raising

All staff will complete a training session covering.

- physical abuse: including hitting, slapping, punching, burning, misuse of medication, inappropriate restraint.
- sexual abuse: including rape, indecent assault, inappropriate touching, exposure to pornographic material.
- psychological or emotional abuse: including belittling, name calling, threats of harm, intimidation, isolation.
- financial or material abuse: including stealing, selling assets, fraud, misuse or misappropriation of property, possessions or benefits.
- neglect and acts of omission: including withholding the necessities of life such as medication, food or warmth, ignoring medical or physical care needs.
- discriminatory abuse: including racist, sexist, that based on a person's disability and other forms of harassment, slurs or similar treatment.
- institutional or organisational: including regimented routines and cultures, unsafe practices, lack of person-centred care or treatment.
- Abuse may be carried out deliberately or unknowingly. Abuse may be a single act or repeated acts.

- People who behave abusively come from all backgrounds and walks of life. They may be doctors, nurses, social workers, advocates, staff members, volunteers or others in a position of trust. They may also be relatives, friends, neighbours or people who use the same services as the person experiencing abuse.

What is the Prevent Duty?

The Duty is part of the government's counter-terrorism strategy, CONTEST. Its aim is to stop people becoming terrorists or supporting terrorism.

What are Fundamental British Values?

In its Prevent Duty strategy the government has defined Fundamental British Values as:

Democracy

The rule of law

Individual liberty

Mutual respect

Tolerance of those with different faiths and beliefs

Blank

Procedures

1. **Introduction**

Keith Cook Training Limited provides a Training and Assessment service to Employed and Unemployed people. These procedures have been designed to ensure the welfare and protection of any adult who accesses services provided by Keith Cook Training Limited. The procedures recognise that adult abuse can be a difficult subject for workers to deal with. Keith Cook Training Limited is committed to the belief that the protection of vulnerable adults from harm and abuse is everybody's responsibility, and the aim of these procedures is to ensure that all managers, trustees of the organisation, management committee members, staff and volunteers act appropriately in response to any concern around adult abuse.

2. **Preventing abuse**

Keith Cook Training Limited is committed to putting in place safeguards and measures to reduce the likelihood of abuse taking place within the services it offers and that all those involved within Keith Cook Training Limited will be treated with respect.

Therefore, this policy needs to be read in conjunction with the following policies:

- Equal Rights and Diversity
- Volunteers
- Complaints
- Whistle Blowing
- Confidentiality
- Disciplinary and Grievance
- Data Protection
- Recruitment and Selection
- Any other policies which are relevant that the organisation has in place (e.g. Challenging Behaviour, Handling Money)

Keith Cook Training Limited is committed to safer recruitment policies and practices for paid staff, trustees and volunteers. This may include CRB disclosures for staff and volunteers, ensuring references are taken up and adequate training on Safeguarding Adults is provided for staff and volunteers.

Management committee members/trustees will be required to provide two references and where appropriate have a Criminal Records Bureau disclosure.

The organisation will work within the current legal framework for reporting staff or volunteers that are abusers.

Service users will be encouraged to become involved with the running of the organisation. Information will be available about abuse and the complaints policy and Safeguarding Adults policy statement will be available to service users and their carers/families.

3. **Recognising the signs and symptoms of abuse**

Keith Cook Training Limited is committed to ensuring that all staff, the management committee, trustees and volunteers undertake training to gain a basic awareness of signs and symptoms of abuse. Keith Cook Training Limited will ensure that the Designated Named Person and other members of staff, trustees and volunteers have access to training around Safeguarding Adults.

- "Abuse is a violation of an individual's human and civil rights by any other person or persons" (No Secrets: Department of Health, 2000)
- **Abuse includes:**

  Discriminatory
  Psychological
  Financial or material
  Organisational
  Neglect and acts of omission
  Physical
  Sexual
  Domestic
  Modern slavery
  Self-neglect

4. Designated Named Person for safeguarding adults

Keith Cook Training Limited has an appointed individual who is responsible for dealing with any Safeguarding Adults concerns. In their absence, a deputy will be available for workers to consult with. The Designated Named Person(s) for Safeguarding Adults within Keith Cook Training Limited is/are:

George Walton
01509 600330
07866 360214

Michael Halliday
01509 600330
07714 207750

Should either of these named people be unavailable then management committee members, trustees, staff or volunteers should contact Adult Social Care Direct directly. See below for contact details.

The roles and responsibilities of the named person(s) are:

- To ensure that all staff including volunteers and trustees are aware of what they should do and who they should go to if they have concerns that a vulnerable adult may be experiencing or has experienced abuse or neglect.
- To ensure that concerns are acted on, clearly recorded and referred to an Adult Social Care Direct team or to the allocated social worker/care manager where necessary.
- To follow up any referrals and ensure the issues have been addressed.
- consider any recommendations from the Safeguarding Adults process.
- To reinforce the utmost need for confidentiality and to ensure that staff and volunteers are adhering to good practice with regard to confidentiality and security. This is because it is around the time that a person starts to challenge abuse that the risks of increasing intensity of abuse are greatest.
- to ensure that staff and volunteers working directly with service users who have experienced abuse, or who are experiencing abuse, are well supported and receive appropriate supervision.
- if appropriate staff or volunteers will be given support and afforded protection if necessary, under the Public Interest Disclosure Act 1998: they will be dealt with in a fair and equitable manner and they will be kept informed of any action that has been taken and it's outcome

5. Responding to people who have experienced or are experiencing abuse.

Keith Cook Training Limited recognises that it has a duty to act on reports, or suspicions of abuse or neglect. It also acknowledges that taking action in cases of adult abuse is never easy.

How to respond if you receive an allegation:

- Reassure the person concerned.
- Listen to what they are saying.
- Record what you have been told/witnessed as soon as possible.
- Remain calm and do not show shock or disbelief.
- Tell them that the information will be treated seriously.
- Don't start to investigate or ask detailed or probing questions.
- Don't promise to keep it a secret.

If you witness abuse or abuse has just taken place the priorities will be:

- To call an ambulance if required
- To call the police if a crime has been committed.
- To preserve evidence
- To keep yourself, staff, volunteers and service users safe
- To inform the Designated Named Person in your organisation
- To record what happened in name of place/file/log where safeguarding adults' concerns will be recorded

All situations of abuse or alleged abuse will be discussed with the Designated Named Person or their deputy. If a member of the management committee, a trustee, staff member or volunteer feels unable to raise this concern with the Designated Named Person or their deputy then concerns can be raised directly with Adult Social Care Direct. The alleged victim will be told that this will happen. This stage is called the alert.

If it is appropriate and there is consent from the individual, or there is a good reason to override consent, such as risk to others, a referral (alert) will be made to Adult Social Care Direct team.

If the individual experiencing abuse does not have capacity to consent a referral will be made without that person's consent, in their best interests.
The Designated Named Person may take advice at the above stage from Adult Social Care Direct and/or the Safeguarding Adults Unit and/or other advice-giving organisations such as Police.

Adult Social Care Direct
Phone: **0116 305 0004**
Address: 52 King Street, Leicester LE1 6RL
Available: Monday-Friday 8am-5.30pm

Safeguarding Adults Unit
Phone: 0116 454 1004
Available: Monday, Wednesday and Friday morning, 9.30am-12.00noon.
Please note that this is an advice service ONLY. All alerts should be raised with Adult Social Care Direct.

Leicestershire Police
Phone: 0116 248 2404
(Ask for Local Area Police Station or MAPPA Administration Officer)

Raising a Safeguarding Adults Alert

All safeguarding adults' alerts (referrals) should be made by telephone to the Adult Social Care Direct Team at the Shielfield Centre Monday to Friday 8.00am till 6.00 pm

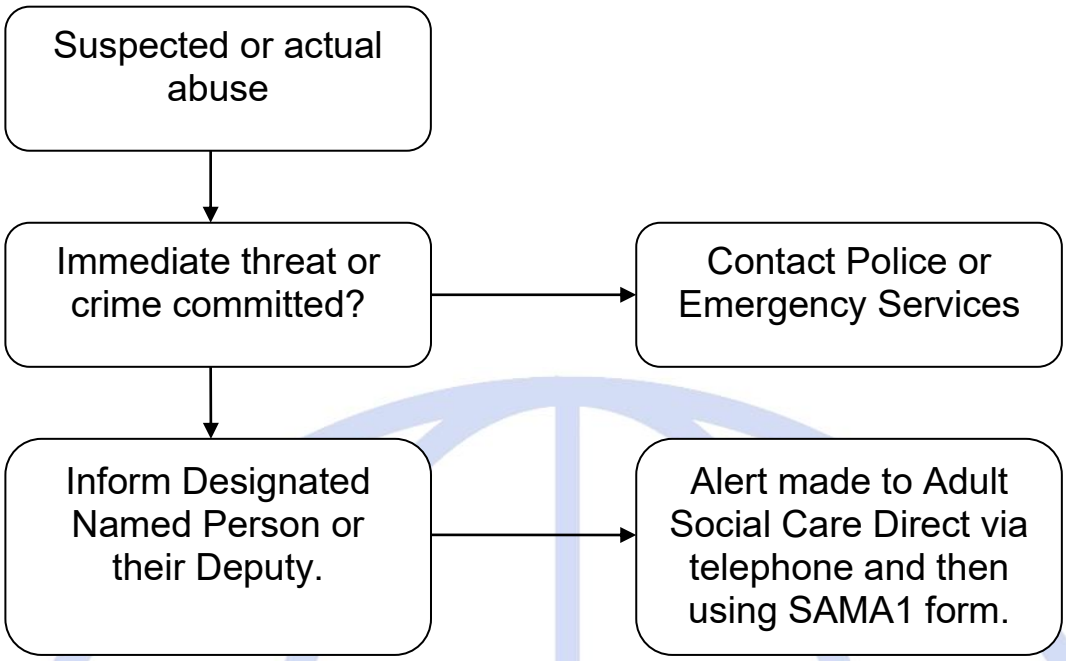
Phone: 0116 252 7004

Posted: Leicester City Adult Social Care 1 Grey Friars Leicester LE1 5PH
Available: Monday-Friday 8am-6pm

In an emergency situation, outside of these times please contact the Emergency Duty team on 0191 232 8520

You should ask to make a safeguarding adults alert.

The telephone call should be followed up in writing to the Adult Social Care Direct team outlining concerns using a Safeguarding Adults Multi-Agency Alert form (SAMA1). This form can be found at the end of these procedures (Annex 1). This should be faxed to Adult Social Care Direct team after ensuring that the fax is in a safe haven by confirming the fax number and ringing after sending to ensure its safe arrival or sent by secured post in a double envelope – marked strictly confidential.



A Safeguarding Adults Manager (a Team Manager from Adult and Culture Services) will then decide if the safeguarding process should be instigated or if other support/services are appropriate. Feedback will be given to the person who raised the safeguarding adults alert.

If the Safeguarding Adults Manager decides the safeguarding process needs to be instigated this will then lead to the implementation of the next stages of Keith Cook Training Ltd Policy and Procedures?

The Designated Named Person will have an overview of this process so they can explain it to the person concerned and offer all relevant support to the person and process. This could be practical support e.g. providing a venue, or information and reports and emotional support.

Information should be provided to the individual. This could be about other sources of help or information that could enable them to decide what to do about their experience, enable them to recover from their experience and enable them to seek justice.

6. Managing allegation made against member of staff or volunteer.

Keith Cook Training Limited will ensure that any allegations made against members or member of staff will be dealt with swiftly.

Where a member of staff/volunteer is thought to have committed a criminal offence the police will be informed. If a crime has been witnessed the police should be contacted immediately.

The safety of the individual(s) concerned is paramount. A risk assessment must be undertaken immediately to assess the level of risk to all service users posed by the alleged perpetrator. This will include whether it is safe for them to continue in their role or any other role within the service whilst the investigation is undertaken.

The Designated Named Person will liaise with Adult Social Care Direct to discuss the best course of action and to ensure that the Keith Cook Training Limited's disciplinary procedures are coordinated with any other enquiries taking place as part of the ongoing management of the allegation.

Keith Cook Training Limited has a whistle blowing policy and staff are aware of this policy. Staff will be supported to use this policy.

7. Recording and managing confidential information

Keith Cook Training Limited is committed to maintaining confidentiality wherever possible and information around Safeguarding Adults issues should be shared only with those who need to know. For further information, please see Keith Cook Training Limited's confidentiality policy.

All allegations/concerns should be recorded in name of place/file/log where safeguarding adults' concerns will be recorded. The information should be factual and not based on opinions, record what the person tells you, what you have seen and witnesses if appropriate.

The information that is recorded will be kept secure and will comply with data protection.

This information will be secured in a locked room in the organisation. Access to this information will be restricted to the Designated Named Person.

8. Disseminating/Reviewing policy and procedures

This Safeguarding Adults Policy and Procedure will be clearly communicated to staff, trustees, volunteers, service users, parents and carers. The Designated Named Person will be responsible for ensuring that this is done.

The Safeguarding Adults Policy and Procedures will be reviewed annually by Keith Cook Training Ltd. The Designated Named Person for Safeguarding Adults will be involved in this process and can recommend any changes. The Designated Named Person will also ensure that any changes are clearly communicated to staff, trustees and volunteers. It may be appropriate to involve service users in the review and service users and parents/carers need to be informed of any significant changes.

Safeguarding Adults Multi-Agency Alert Form

Reference: SAMA1

This form is to be used to notify Adult and Culture Services Directorate/ Adult Social Care

Person completing the form: **Organisation Name:** **Service / Ward Name:** **Phone contact details:** **Date of Notification to Adult Social Care Direct:**

Details of incident/suspected or actual abuse **To be completed by the manager or lead officer within the organisation responsible for safeguarding adults**	
Date of alleged incident/harm: **Time of alleged incident/harm:**	**Area where incident/harm took place:** **Who reported the alert:** **Date:**
Who was involved:	
Details of Alleged Victim **Name:** **Address:** **Date of Birth:** **Phone:**	**Name and address of GP:** **Ethnic Origin:** **Nature of alleged victims' vulnerability:** **Any other details** (e.g. communication needs)**:**
Details of Alleged Perpetrator **Name:** **Address:** **Date of Birth:** **Phone Contact:** **If the alleged perpetrator is a staff member, please provide staff details** (E.g. job role, employer, address of place of work)	**Ethnic Origin:** **Relationship to victim:** **Are they a vulnerable adult? Yes/No** **Alleged perpetrators vulnerability** (if applicable)**:** **Any other details:**
Have you made the victim aware that details of the incident are being recorded and will be investigated? **Yes/No**	

If not, why not?

Type of Abuse (Please tick one or more)

✓			
Sexual		**Physical**	
Emotional		**Neglect or omission**	
Psychological		**Financial/Material**	
Discriminatory Abuse		**Institutional**	
Other i.e. suspicious death of a service user			

Description of alleged incident / alleged harm, detailing all people involved including witnesses.
On this page, please give a detailed description of the incident (please include times) and any other comments you feel are relevant. If necessary, attach further pages.

What action did you take immediately after the incident/allegation of harm (E.g. administered first aid, asked perpetrator to leave, took victim to secure area)

Were the Police called: Yes / No	**Were any other emergency services called:** If yes, which service(s)? **Yes / No**
Names and badge numbers of Police:	**Outcome**: (Response time, taken to hospital etc)
Are there any other Agencies involved? Yes/No	**Please provide details of agencies:**
Are there any capacity issues? Yes/ No	**Please provide details:**
Has the victim made any previous referrals/alerts? Yes/No	**Please provide details** (e.g. dates, type of abuse)**:**

Is the victim in immediate danger of further abuse? Yes/No	**Have any immediate actions been identified to reduce the potential for further abuse? Yes/No**
Has an initial assessment been made to determine further potential risk to the victim? Yes/No	**What actions have been taken to reduce the potential for further abuse?**
Are there any risks to others? Yes/No (Vulnerable adults, children)	**Please provide details** (include who this information has been shared with – e.g. Children's Social Care, Police)**:**
Signed:	**Date:** **Time:**
This form must be sent to the Adult Social Care Direct team / or allocated social worker within 24 hours of the suspected or actual abuse, or as soon as possible after being made aware. **This form can be Posted: : Leicester City Adult Social Care 1 Grey Friars Leicester LE1 5PH** **This must be accompanied a phone call to the Adult Social Care Direct Team (0116 252 7004)/allocated social worker advising alert is being sent.**	

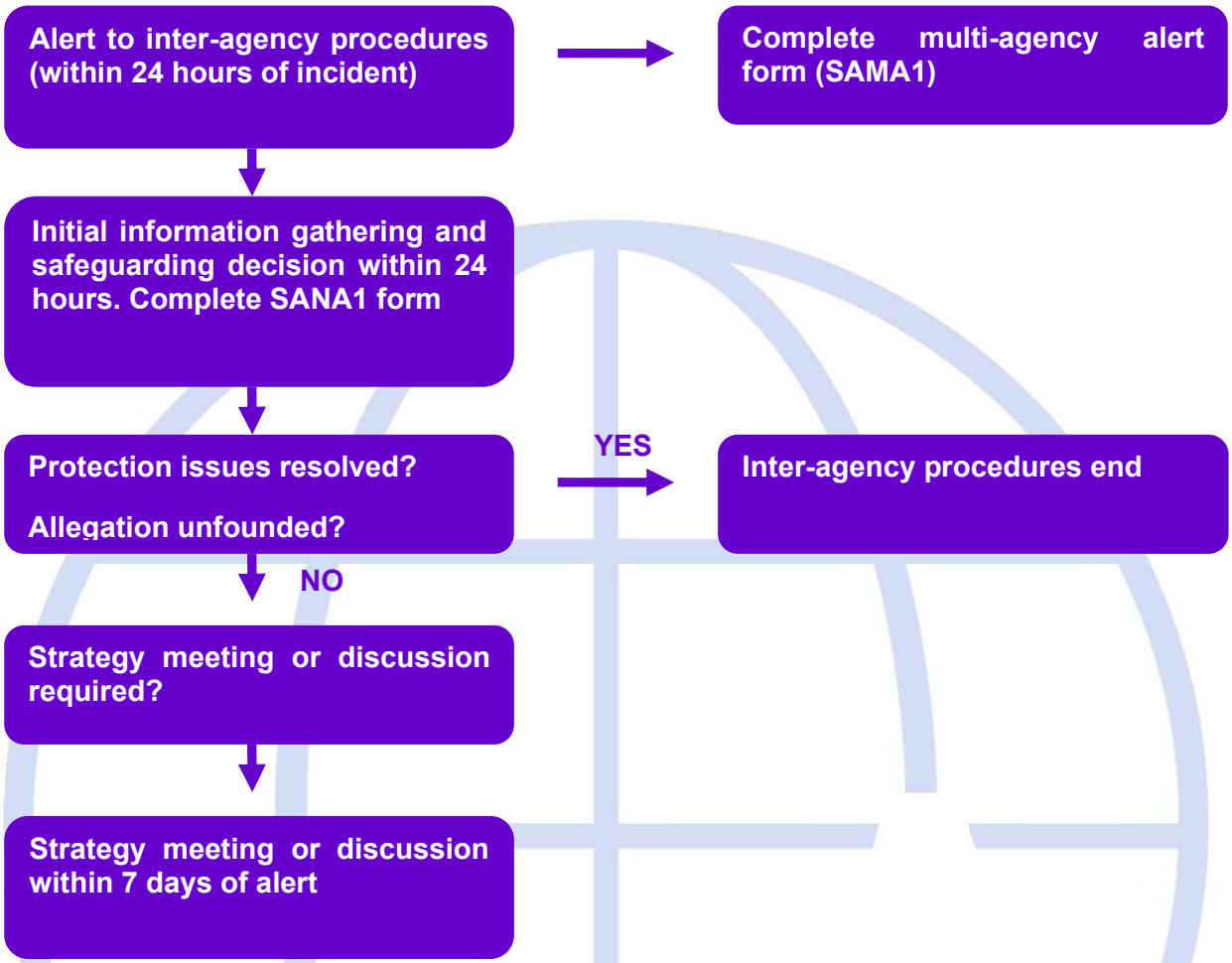
This is a confidential document and should be stored securely according to your own organisation's procedures. It is your responsibility to ensure that this is done.

Decision by Safeguarding Manager (Adult and Culture Services Directorate Only) Safeguarding Alert Yes / No

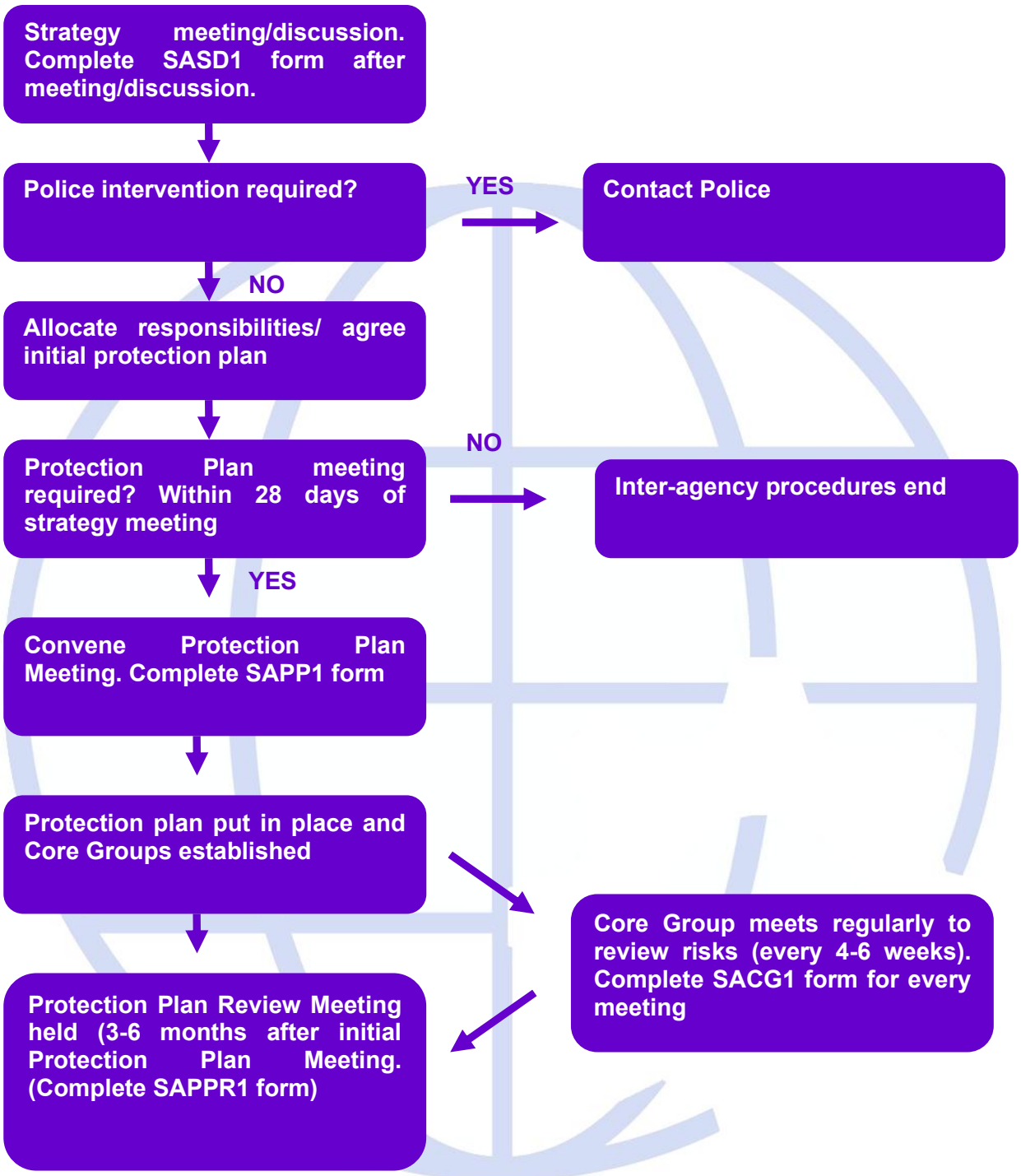
If No – please give reasons for decision.

Part 9 – Decision Protection Strategy Plans with Policies developed from these Plans.

Decision and strategy stage 1



Strategy and Protection Plan Stage 2



Sustainable Development Policy

- Purpose of policy:

To define the Companies commitment to sustainable development

- Approval for this policy given by:

Management

- Responsibility for its update:

All Sections
The Centre Environment
Education for Sustainable Development
Working with the Community
Skills, HE and Business Development

Date of approval: April 2012
Date of review: April 2025

Policy applies to: To all candidates Definition and Staff this policy adopts the definition of sustainable development outlined in The Brundtland Report:

"Development which meets the needs of the present without compromising the ability of future generations to meet their own needs".

World Commission on Environment and Development (1987)

Sustainable development is the simple idea of ensuring a better quality of life for everyone, both now and for generations to come. A key strategic objective of the Company is:

"To secure the Company's commitment to sustainable practice".

We share the principles to support the implementation of sustainable development.

These are to:
- Understand and balance the environmental, social and economic impacts of the decisions we make.
- Live within environmental limits, ensuring the prudent use of natural resources and the prevention of pollution.
- Take a long-term perspective in all that we do.
- Ensure a 'whole Company approach' to sustainable development.
- Continual improvement, through setting objectives and targets and monitoring and review.

Sustainable Development Policy

As a Company within the local East Midlands community, the Company has a responsibility to be central in delivering the sustainability message to that community, not only through the courses that we run but also in the way that we behave as a Company. We see it as essential that our actions as a Company; help to transform the future lives of our Candidates through brighter continued employment prospects, play a part in transforming all of our futures through responsible environmental management and support sustainable development within the community.

The Company's responsibility, therefore, is outlined in the following three sections:

- Section 1 Sustainable Development: The Centre Environment
- Section 2 Education for Sustainable Development
- Section 3 Sustainable Development: Working with the Community

The Centre Environment

The Company adopts the following definition of the environment:

"Surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans and their interrelation"

ISO 14001:2004 Definition Keith Cook Training Limited recognises that the nature and scale of its activities impacts on the environment and that it has a responsibility to manage its activities in a way that reduces negative environmental impacts and increases positive impacts. The Company is, therefore, committed to carbon reduction and improving its environmental performance though an environmental management system. The implementation of this policy will enable it to do so. The following areas of environmental management fall within the scope of this policy.

- Use of energy
- Use of water
- Use of resources
- Emissions from transport
- Waste
- Contamination of land
- Loss of biodiversity In order to meet our environmental responsibilities, and to reduce our carbon footprint, we will engage in the following actions:
- Comply with all relevant legal requirements and other management standards and guidelines.
- Develop, implement and maintain an environmental management system, aiming to meet the requirements for certification to the ISO14001 standard.
- Optimise energy efficiency to reduce emissions of greenhouse gases • Optimise water use efficiency.
- Be efficient in the use of resources.
- Reduce the negative environmental impacts of travel.
- Increase reuse and recycling and reduce waste.
- Prevent pollution and contamination of land and water and continually improve our environmental performance.
- Manage and improve the biodiversity value of the Centre.
- Give appropriate consideration to environmental criteria when purchasing products and services and where possible select contractors and suppliers who can demonstrate environmental management and performance in line with this policy.
- Raise awareness of appropriate environmental issues amongst members of the Company, and provide relevant training.
- Use internal audits to monitor compliance with the environmental management system.
- Increase general awareness of environmental responsibilities amongst candidates and staff through internal communications, education for sustainable development and staff development.

The implementation of this section of the policy will be the responsibility of Centre, Sustainable Development and Finance who will develop an action plan for improving environmental performance, with measurable indicators where possible, and will report annually on its progress.

Education for Sustainable Development

The Company adopts the following definition of education for sustainable development (KCT):

"The process of acquiring the knowledge, skills and attitudes needed to build local and global societies that are just, equitable and living within the environmental limits of our planet, both now and in the future."

Sustainable Development Education Network definition

The LSIS *Sustaining our Future Framework* Positions Education for Sustainable Development in the context of the significant environmental, social and economic challenges we face as individuals, as a sector and as a nation.

Education for Sustainable Development is also encompassed within the key strategic objective of the Company:

"To provide a course portfolio that anticipates and meets the needs of candidates, employers and other stakeholders and addresses local, regional and national priorities".

The Company aims to take a holistic approach to equip candidates with the knowledge, skills and attitudes to be effective citizens in this changing world. This will involve not only what the candidates learn within their formal courses and the way teaching and learning is delivered, but also the wider informal Company initiatives, events and culture that will influence candidates and staff to live and work more sustainably. In order to meet this aim, we will:

- Identify any additional qualifications offered in sustainable development and/or environmental issues. Develop the curriculum portfolio, as appropriate, to equip learners to contribute to the low carbon economy.
- Map where KCT is already integrated in courses and expand and contextualise the delivery of KCT for specific curriculum and vocational areas.
- Promote projects and competitions to raise awareness of SD issues and showcase candidates' work.
- Promote the culture of the Sustainable Company Community through induction and tutorial.
- Develop KCT as a vehicle to enhance every person Matters outcomes, particularly healthy lifestyles, making a positive contribution and achieving economic well-being.
- Ensure that teaching methods are environmentally conscious and encourage the use of online materials, the VLE and other strategies to reduce the need for travel and paper.
- Develop the use of the centre and facilities as a teaching resource in liaison with course areas.
- Develop a resource base of SD teaching/learning materials on the VLE, Staff Information System and in the library.
- Develop the inclusion of KCT in cross Company monitoring and planning systems, for example, course team meetings and the self-assessment reporting.
- Use external benchmarking, for example The Reaching Forward Index, to set targets and monitor progress against national criteria.
- Work with the Candidates/Employers and Course Instructors to support candidate led initiatives, encourage active participation and link to national or international sustainability events and themes.
- Identify opportunities for volunteering in Sustainable Development and the environment within relevant courses.
- Provide KCT staff development opportunities and ongoing advice and support for staff delivering KCT The implementation of this section of the policy will be the responsibility of the Sustainable Development Manager, who will develop an action plan and report annually on its progress,

Working with the Community

The Company adopts the following definition of a sustainable community:

"*Sustainable communities are places where people want to live and work, now and in the future. They meet the diverse needs of existing and future residents, are sensitive to their environment, and contribute to a high quality of life."* (2003 Sustainable Communities Plan).

Working towards a sustainable community is encompassed within the key strategic objective of the Company:

"To develop and maintain partnership arrangements which deliver measurable and positive benefits to the Company and the community we serve".

The Company works with and within the community.

Within the organisation, itself the Company aims to develop its strong 'community' ethos, from how we engage with candidates and staff through to how we run our operations. Within the local community, the Company will position itself as an exemplar organisation and work with local stakeholders towards a sustainable community. Within the region, it aims to be a proactive and responsive stakeholder in promoting sustainable development. In order to meet these aims we will:

- Communicate effectively with our local community stakeholders, including employers, to increase the involvement of the Company and its candidates in contributing to the sustainable community.
- As a stakeholder, the Company will maintain and develop appropriate local and regional partnerships and networks - for example between Companies, schools, learning providers, local authorities and higher education.
- Encourage candidates to organise or contribute to local community events and to undertake volunteering as part of a community commitment to sustainable development.
- Support local markets, ethical and fair trade and local initiatives within the community where appropriate
- Increase access to facilities for local community agencies and groups to make the best use of resources.
- Use external benchmarking, for example the LSIS Reaching Forward Index, to set targets and monitor progress against national criteria.

Animal Welfare Policy

Keith Cook Training Limited (KCTL) does not allow mistreatment of animals. All animals are to be treated with utmost respect and care. Any employee who mistreats an animal will be terminated immediately and without notice. Any individual who witnesses the mistreatment of animals by another individual is also subject to termination unless he/she reports the mistreatment to (KCTL) during that current working day or by calling the confidential toll-free number that has been posted for this purpose. (KCTL) reserves the right to press criminal charges against employees who mistreat animals.

The mistreatment of an animal is defined as hitting, inappropriate electrical prodding, kicking, or performing any other action that may cause undue stress or pain to the animal.
Mistreatment also includes the beating or hitting of non-ambulatory or “downer” animal.

Anyone signing a company contract must follow these Policies, the Employee/Sub Contractor is stating that I understand these procedures and will abide by this policy. If the Employee/Sub Contractor does not abide by the policy, the Employee/Sub Contractor will be terminated and will face possible criminal charges.

MALPRACTICE & MALADMINISTRATION POLICY

(Also refer to appendices for specific accrediting body additional information)

Introduction

This policy is aimed at our customers, including learners, who are delivering/registered on Keith Cook Training Limited (KCTL) programmes or courses, approved qualifications or units within or outside the UK and who are involved in suspected or actual malpractice/maladministration. It is also for use by our staff to ensure they deal with all malpractice and maladministration investigations in a consistent manner.

It sets out the steps our centre, and learners or other personnel must follow when reporting suspected or actual cases of malpractice/maladministration and our responsibilities in dealing with such cases. It also sets out the procedural steps we will follow when reviewing the cases.

Centre’s responsibility

It is important that all staff involved in the management, assessment and quality assurance of our qualifications, and learners, are fully aware of the contents of the policy and we have arrangements in place to prevent and investigate instances of malpractice and maladministration.

Malpractice means any act, default or practice (whether deliberate or resulting from neglect or default) which is a breach of SQA/ Awarding Organisation requirements including any act, default or practice which:

- compromises, attempts to compromise, or may compromise the process of assessment, the integrity of any SQA/Awarding Organisation qualification, or the validity of a result or certificate; and/or
- damages the authority, reputation or credibility of SQA/ Awarding Organisation or any officer, employee or agent of SQA/ Awarding Organisation.

Some incidents of malpractice are unintentional. We define unintentional malpractice as 'maladministration', which includes incidents that arise due to ignorance of SQA/Awarding Organisation requirements, carelessness or neglect in applying the requirements.

.

Examples of maladministration

- Persistent failure to adhere to our learner registration and certification procedures.
- Persistent failure to adhere to our centre recognition and/or qualification requirements and/or
- Associated actions assigned to the centre
- Late learner registrations (both infrequent and persistent)

- Unreasonable delays in responding to requests and/or communications from KCTL
- Inaccurate claim for certificates
- Failure to maintain appropriate auditable records, e.g. certification claims and/or forgery of evidence
- Withholding of information, by deliberate act or omission, from us which is required to assure Active

Examples of malpractice

- Failure to carry out internal assessment, internal moderation or internal verification in accordance with our requirements
- Deliberate failure to adhere to our learner registration and certification procedures.
- Deliberate failure to continually adhere to our centre recognition and/or qualification approval requirements or actions assigned to your centre
- Deliberate failure to maintain appropriate auditable records, e.g. certification claims and/or forgery of evidence
- Fraudulent claim(s) for certificates
- Intentional withholding of information from us which is critical to maintaining the rigor of quality assurance and standards of qualifications
- Collusion or permitting collusion in exams/assessments
- Learners still working towards qualification after certification claims have been made
- Plagiarism by learners/staff
- Copying from another learner (including using ICT to do so).

Process for making an allegation of malpractice or maladministration.
Anybody who identifies or is made aware of suspected or actual cases of malpractice or maladministration at any time must immediately notify the Directors of Academy of Learning Ltd. In doing so they should put them in writing/email and enclose appropriate supporting evidence.

- All allegations must include (where possible):
- Learner's name and KCTL registration number
- KCTL's staff members name and job role - if they are involved in the case
- Details of the course/qualification affected, or nature of the service affected
- Nature of the suspected or actual malpractice and associated dates details and outcome of any initial investigation carried out by the centre or anybody else involved in the case, including any mitigating circumstances.

The Directors will then conduct an initial investigation prior to ensure that staff involved in the initial investigation are competent and have no personal interest in the outcome of the investigation.
In all cases of suspected malpractice and maladministration reported we'll protect the identity of the 'informant' in accordance with our duty of confidentiality and/or any other legal duty.
Confidentiality and whistle blowing.

Sometimes a person making an allegation of malpractice or maladministration may wish to remain anonymous. Although it is always preferable to reveal your identity and contact details to us; however, if you are concerned about possible adverse consequences, you may request that the Directors do not divulge your identity.

While we are prepared to investigate issues which are reported to us anonymously, we shall always try to confirm an allegation by means of a separate investigation before taking up the matter with those the allegation relates.

Responsibility for the investigation

In accordance with regulatory requirements all suspected cases of maladministration and malpractice will be examined promptly by KCTL to establish if malpractice or maladministration has occurred and will take all reasonable steps to prevent any adverse effect from the occurrence as defined by Ofqual. We will acknowledge receipt, as appropriate, to external parties within 48 hours.

Our Director will be responsible for ensuring the investigation is carried out in a prompt and effective manner and in accordance with the procedures in this policy and will allocate a relevant member of staff to lead the investigation and establish whether or not the malpractice or maladministration has occurred, and review any supporting evidence received or gathered by KCTL.

Notifying relevant parties

Where applicable, our director will inform the appropriate regulatory authorities if we believe there has been an incident of malpractice or maladministration which could either invalidate the award of a qualification or if it could affect another awarding organisation.

Where the allegation may affect another awarding organisation and their provision, we will also inform them in accordance with the regulatory requirements and obligations imposed by the regulator Ofqual. If we do not know the details of organisations that might be affected, we will ask Ofqual to help us identify relevant parties that should be informed.

Investigation timelines and summary process

We aim to action and resolve all stages of the investigation within 10 working days of receipt of the allegation.

The fundamental principle of all investigations is to conduct them in a fair, reasonable and legal manner, ensuring that all relevant evidence is considered without bias. In doing so investigations will be based around the following broad objectives:

- To establish the facts relating to allegations/complaints in order to determine whether any irregularities have occurred.
- To identify the cause of the irregularities and those involved.
- To establish the scale of the irregularities.
- To evaluate any action already taken
- To determine whether remedial action is required to reduce the risk to current registered learners and to preserve the integrity of KCTL and the qualification.
- To identify any adverse patterns or trends.

The investigation may involve a request for further information from relevant parties and/or interviews with personnel involved in the investigation. Therefore, we will:

- Ensure all material collected as part of an investigation must be kept secure.
- If an investigation leads to invalidation of certificates, or criminal or civil prosecution, all records and original documentation relating to the case will be retained until the case and any appeals have been heard and for six years thereafter.
- Expect all parties, who are either directly or indirectly involved in the investigation, to fully co-operate with us.

Either at notification of a suspected or actual case of malpractice or maladministration and/or at any time during the investigation, we reserve the right to withhold a learner's, and/or cohort's, results.

Where a member of KCTL's staff or an KCTL Associate is under investigation we may suspend them or move them to other duties until the investigation is complete.

Throughout the investigation our Director will be responsible for overseeing the work of the investigation team to ensure that due process is being followed, appropriate evidence has been gathered and reviewed and for liaising with and keeping informed relevant external parties.
Investigation report.

After an investigation, we'll produce a draft report for the parties concerned to check the factual accuracy. Any subsequent amendments will be agreed between the parties concerned and ourselves. The report will:

- Identify where the breach, if any, occurred.
- Confirm the facts of the case.
- Identify who is responsible for the breach (if any)
- Confirm an appropriate level of remedial action to be applied.

We'll make the final report available to the parties concerned and to the regulatory authorities and other external agencies as required.

If it was an independent/third party that notified us of the suspected or actual case of malpractice, we'll also inform them of the outcome – normally within 10 working days of making our decision - in

doing so we may withhold some details if to disclose such information would breach a duty of confidentiality or any other legal duty.

If it's an internal investigation against a member of our staff the report will be agreed by the Managing Director, along with the relevant internal managers and appropriate internal disciplinary procedures will be implemented.

Investigation outcomes

If the investigation confirms that malpractice or maladministration has taken place we will consider what action to take in order to:

- Minimise the risk to the integrity of certification now and in the future.
- Maintain public confidence in the delivery and awarding of qualifications.
- Discourage others from carrying out similar instances of malpractice or maladministration.
- Ensure there has been no gain from compromising our standards.

The action we take may include:

- Imposing actions in order to address the instance of malpractice/maladministration and to prevent it from reoccurring
- In cases where certificates are deemed to be invalid, inform the Awarding Organisation concerned and the regulatory authorities why they're invalid and any action to be taken for reassessment and/or for the withdrawal of the certificates. We'll also let the affected learners know the action we're taking and that their original certificates are invalid and ask – where possible – to return the invalid certificates to KCTL.
- Informing relevant third parties (e.g. funding bodies) of our findings in case they need to take relevant action in relation to the centre.

In addition, to the above the Director will record any lessons learnt from the investigation and pass these onto relevant internal colleagues to help prevent the same instance of maladministration or malpractice from reoccurring.

If the relevant parties wish to appeal against our decision to impose sanctions, please refer to our Complaints Procedure.

Where an investigation of suspected malpractice is carried out, KCTL will retain related records and documentation for three years for non-regulated qualifications and six years for regulated qualifications. Records will include any work of the candidate and assessment or verification records relevant to the investigation.
In the case of an appeal to any awarding or accrediting body (e.g. SQA) against the outcome of a malpractice investigation, assessment records will be retained for six years.

In an investigation involving a potential criminal prosecution or civil claim, records and documentation will be retained for six years after the case and any appeal has been heard. If KCTL is any doubt about whether criminal or civil proceedings will take place, it will keep records for the full six year period.

SQA Specific in addition to above:

We have the right to appeal a decision where a case of reported malpractice by our centre has been confirmed through investigation by SQA.
We also have the right to appeal a decision in the case of suspected malpractice by a candidate reported by our centre to SQA.
Candidates have the right to appeal to SQA:

- our centre has conducted an investigation, the candidate disagrees with the outcome and has exhausted our centre's appeals process,
- SQA has asked our centre to conduct an investigation and the candidate disagrees with the outcome and has exhausted our centre's appeals process, and
- SQA has conducted an investigation and the candidate disagrees with the decision

For regulated qualifications only:
Our centre and our candidates have the right to request a review by the appropriate regulator (SQA Accreditation, Ofqual or Qualifications Wales) of the awarding organisation process in reaching a decision in an appeal of a malpractice decision.

Please refer to: The Appeals Process: Information for SQA Centres

Recognition of Prior Learning (RPL)

Is a method of assessment [leading to the award of a qualification] that considers whether learners can demonstrate that they can meet the assessment requirements for a unit through knowledge, understanding or skills they already possess and do not need to develop through a course of learning.

Note: RPL should not be confused with exemption, unit equivalency or credit accumulation and transfer.

For further information about credit accumulation please see the Credit Accumulation and Transfer Policy.

RPL enables recognition of achievement from a range of activities using any appropriate assessment methodology.

Provided that the assessment requirements of a given unit or qualification have been met, the use of RPL is acceptable for accrediting a unit, units or a whole qualification. Partial unit completion is not acceptable. Evidence of learning must be:

- Valid1
- Reliable.

KCTL encourages the use of RPL where it is of value to the centre and learners in facilitating assessment.

KCTL which uses RPL must follow these principles and keep appropriate records.

I. Conflict of Interest Policy

A possible conflict of interest exists when a director has a material personal interest, either direct or indirect, in a proposed transaction involving this organization. When a director has an interest in a transaction being considered by the organization, the director should disclose that conflict before the board of directors or staff member takes action on the matter.

Any board member having a conflict of interest will not vote or use his or her personal influence on the matter and will not be present when the matter is discussed by the board. The minutes of the meeting will reflect that a disclosure was made, and the abstention from voting.

This policy also will apply to immediate family members, the organization's committees, and its volunteer association. Directors, committee members, staff members, and officers of the volunteer association will be required to attest annually to their familiarity with this policy and to provide information concerning any possible conflict of interest so that disclosure, if necessary, is made.

Staff members and their immediate families will not benefit materially from the organization beyond receipt of salaries, fringe benefits, and reimbursement for authorized expenses.

II. Definition of Material Personal Interest

A material personal interest is:

1. An ownership or investment interest in any entity with which this organization has a transaction or arrangement.
2. A compensation arrangement with the organization or with any entity or individual with which the organization has a transaction or arrangement; or
3. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the organization is negotiating a transaction or arrangement. Compensation includes direct and indirect remuneration as well as gifts, favours, and non-financial benefits that are not insubstantial.

III. Procedures

1. The interested director(s) will disclose to the Board, preferably in writing, the material facts as to his or her material personal interest in the transaction and in any corporation, partnership, association or other organization involved in the transaction prior to the meeting at which the Board acts upon the transaction.
2. The interested director(s) will absent himself or herself from the meeting while the transaction is discussed and acted upon.
3. A disinterested director, or other disinterested party familiar with the transaction, will present evidence of the fairness of the proposed transaction, such as competitive bids or comparable price quotations.
4. The vote of a majority of the disinterested directors participating in the meeting and constituting a quorum, after reaching a decision regarding whether the proposed transaction is fair to the organization, will be required for approval of the transaction. The minutes for the meeting will reflect that a disclosure of interest was made and that the interested director(s) abstained from voting and was not present during the Board's consideration of the transaction.
5. These procedures (i) will apply to transactions approved after the date of adoption of this policy; (ii) will not apply to reimbursement of expenses actually incurred by any director in the course of performing his or her duties as such; and (iii) may be waived or altered in any particular case by vote of a majority of the full Board of Directors for good cause shown.

IV. Potential Conflict Report

To assist in implementing this Policy, each proposed new Board member will file a Potential Conflict Report in the form of Exhibit A hereto in connection with the selection process. Existing Board members will file a Potential Conflict Report annually, in June, with the Executive Director, whose responsibility it will be to oversee the annual distribution of such forms to existing Board members.

Conflict Report

Please answer all questions. If the answer is “yes,” please explain. An affirmative response does not imply that the relationship is improper or that it should be terminated.

During the past twelve months, have you or any related party [1] had any interest, direct or indirect, in any contract or transaction with Arts Organization?

_____.

Do you or any related party have any interest, direct or indirect, in any pending or proposed contract or transaction with Arts Organization?

_____.

Do you or any related party have any other interest, which might conflict, or might be perceived to conflict, with your duty of loyalty to the interests of Arts Organization?

_____.

The answers to the foregoing are accurate to the best of my knowledge and belief, and I will promptly notify the Executive Director of Arts Organization of any change, which would make any of the answers no longer accurate.

Date:_____ Signature:_____

[1] For this purpose, a “related party” is defined as members of your immediate family, which includes your spouse, children, siblings, and parents; estates, trusts, partnerships, limited liability companies, corporations and other entities in which you or any member of your immediate family has a present or vested future beneficial interest or serves as an officer, director, or trustee, other than entities in which you and your immediate family members in the aggregate own less than five percent in value of all traded securities.

Part 10 Information Security Policy

Information Security Policy For Electronic Payments

Keith Cook Training Ltd (KCTL)

(Company Name)

06 /01/2025

(Date)

Contents

1. Introduction
2. Information Security Policy
3. Acceptable Use Policy
4. Disciplinary Action
5. Protect Stored Data
6. Information Classification
7. Access to the sensitive cardholder data
8. Physical Security
9. Protect Data in Transit
10. Disposal of Stored Data
11. Security Awareness and Procedures
12. Network security
13. System and Password Policy
14. Anti-virus policy
15. Patch Management Policy
16. Remote Access policy
17. Vulnerability Management Policy
18. Configuration standards:
19. Change control Process
20. Audit and Log review
21. Secure Application development
22. Penetration testing methodology
23. Incident Response Plan
24. Roles and Responsibilities
25. Third party access to card holder data
26. User Access Management
27. Access Control Policy
28. Wireless Policy

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential company information and must be distributed to all company employees. All company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2. Information Security Policy

KCTL handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

KCTL commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity.
- Limit personal use of KCTL information and telecommunication systems and ensure it doesn't interfere with your job performance.
- KCTL reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
- Do not disclose personnel information unless authorised.
- Protect sensitive cardholder information.
- Keep passwords and accounts secure.
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval.
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended.
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to KCTL's established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and KCTL from illegal or damaging actions by individuals, either knowingly or unknowingly. KCTL will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- Keep passwords secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Because information contained on portable computers is especially vulnerable, special care should be exercised.
- Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of KCTL, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for noncompliance.

5. Protect Stored Data

- All sensitive cardholder data stored and handled by KCTL and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by KCTL for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.,

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3 or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to KCTL if disclosed or modified. Confidential data includes cardholder data.
- Internal Use data might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- Public data is information that may be freely disseminated.

7. Access to the sensitive cardholder data

All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B.
- KCTL will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess.
- KCTL will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- KCTL will have a process in place to monitor the PCI DSS compliance status of the Service provider.

8. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.
- A list of devices that accept payment card data should be maintained.
- The list should include make, model and location of the device.
- The list should have the serial number or a unique identifier of the device.
- The list should be updated when devices are added, removed or relocated.
- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices.
- Personnel using the devices should verify the identity of any third-party personnel claiming to repair or

run maintenance tasks on the devices, install new devices or replace devices.

- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel.
- A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. “Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on KCTL sites. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computer that stores sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

9. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal of Stored Data

- All data must be securely disposed of when no longer required by KCTL, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- KCTL will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated, or pulped so they cannot be reconstructed.
- KCTL will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “To Be Shredded” - access to these containers must be restricted.

11. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with KCTL.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

12. Network security For Card Payments

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal company network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- Stateful Firewall technology must be implemented where the Internet enters KCTL Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented
- KCTL will have firewalls between any wireless networks and the cardholder data environment.
- KCTL will quarantine wireless users into a DMZ, where they will be authenticated and firewalled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorized.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six-month basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- KCTL must quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

Rules	Source IP	Destination IP	Action

13. System and Password Policy

All users, including contractors and vendors with access to KCTL systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO)
- System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1)
- System configurations must include common security parameter settings.
- The systems configuration standard should be applied to any news systems configured.

- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into KCTL network and all unnecessary services and user/system accounts have to be disabled.
- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must me set appropriately on System components.
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to card holder data must have a unique ID.
- All user must use a password to access KCTL network or any other electronic resources
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be setup for new users and the users prompted to change the password on first login.
- Group shared or generic user account or password or other authentication methods must not be used to administer any system components.
- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All non-console administrative access will use appropriate technologies like ssh, vpn etc or strong encryption is invoked before the administrator password is requested.
- System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands
- Administrator access to web-based management interfaces is encrypted using strong cryptography.
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:

a) Be as long as possible (never shorter than 6 characters).
b) Include mixed-case letters, if possible.
c) Include digits and punctuation marks, if possible.
d) Not be based on any personal information.
e) Not be based on any dictionary word, in any language.

- If an operating system without security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

14. Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by KCTL. The preferred application to use is Symantec Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCI DSS requirement 10.7 of 3 months

online and 1 year offline.

- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to modify and any settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch Management Policy

- All Workstations, servers, software, system components etc. owned by KCTL must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Wherever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.
- Any exceptions to this process have to be documented.

16. Remote Access policy

- It is the responsibility of KCTL employees, contractors, vendors, and agents with remote access privileges to KCTL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to KCTL.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong passphrases.
- Vendor accounts with access to KCTL network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to KCTL internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to KCTL network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

17. Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
- As part of the PCI-DSS Compliance requirements, KCTL will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by KCTL by internal staff or a 3rd party vendor and the scan process have to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by KCTL's internal staff. The scan process should include re-scans until passing results are obtained.

18. Configuration standards:

- Information systems that process transmit, or store card holder data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the team responsible for the management of the system in conjunction with the Information Security Office.
- All network device configurations must adhere to KCTL required standards before being placed on the network as specified in KCTL configuration guide. Using this guide, a boilerplate configuration has been created that will be applied to all network devices before being placed on the network.
- Before being deployed into production, a system must be certified to meet the applicable configuration standard.
- Updates to network device operating system and/or configuration settings that fall under KCTL standards are announced by the Information security Office. Updates must be applied within the time frame identified by the Information security Office.
- Administrators of network devices that do not adhere to KCTL standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.
- All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards.

- Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.
- For other devices an audit will be performed quarterly to compare the boilerplate configuration to the configuration currently in place.
- All discrepancies will be evaluated and remediated by Network Administration.

19. Change control Process.

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented. A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see System Development Life Cycle [citation here]).
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see System Development Life Cycle)
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.
- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.
- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see System Development Life Cycle)
- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

20. Audit and Log review

- This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over KCTL network, including the following components:

    - Operating System Logs (Event Logs logs).
    - Database Audit Logs.
    - Firewalls & Network Switch Logs.
    - IDS Logs.
    - Antivirus Logs.
    - CCTV Video recordings.
    - File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
- Review of logs is to be carried out by means of KCTL's network monitoring system (KCTL to define hostname), which is controlled from KCTL console (KCTL to define hostname). The console is installed on the server (KCTL to define hostname / IP address), located within KCTL data centre environment.
- The following personnel are the only people permitted to access log files (KCTL to define which individuals have a job-related need to view audit trails and access log files).
- The network monitoring system software (KCTL to define) is configured to alert KCTL [RESPONSIBLE TEAM] to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:
- A dashboard browser-based interface, monitored by KCTL.
- Email / SMS alerts to KCTL mailbox with a summary of the incident. KCTL also receives details of email alerts for informational purposes.
- The following Operating System Events are configured for logging, and are monitored by the console (KCTL to define hostname):

    a) Any additions, modifications or deletions of user accounts.
    b) Any failed or unauthorised attempt at user logon.
    c) Any modification to system files.
    d) Any access to the server, or application running on the server, including files that hold cardholder data.
    e) Actions taken by any individual with root or administrative privileges.
    f) Any user access to audit trails.
    g) Any creation / deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

- The following Database System Events are configured for logging, and are monitored by the network monitoring system (KCTL to define software and hostname):

    a) Any failed user access attempts to log in to the Oracle database.
    b) Any login that has been added or removed as a database user to a database.

c) Any login that has been added or removed from a role.
d) Any database role that has been added or removed from a database.
e) Any password that has been changed for an application role.
f) Any database that has been created, altered, or dropped.
g) Any database object, such as a schema, that has been connected to.
h) Actions taken by any individual with DBA privileges.

- The following Firewall Events are configured for logging, and are monitored by the network monitoring system (KCTL to define software and hostname):

a) ACL violations.
b) Invalid user authentication attempts.
c) Logon and actions taken by any individual using privileged accounts.
d) Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified).

- The following Switch Events are to be configured for logging and monitored by the network monitoring system (KCTL to define software and hostname):

a) Invalid user authentication attempts.
b) Logon and actions taken by any individual using privileged accounts.
c) Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

- The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (KCTL to define software and hostname):

a) Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
b) Any generic attack(s) not listed in CVE.
c) Any known denial of service attack(s).
d) Any traffic patterns that indicated pre-attack reconnaissance occurred.
e) Any attempts to exploit security-related configuration errors.
f) Any authentication failure(s) that might indicate an attack.
g) Any traffic to or from a back-door program.
h) Any traffic typical of known stealth attacks.

- The following File Integrity Events are to be configured for logging and monitored by (KCTL to define software and hostname):

a) Any modification to system files.
b) Actions taken by any individual with administrative privileges.
c) Any user access to audit trails.
d) Any Creation / Deletion of system-level objects installed by Windows. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

- For any suspicious event confirmed, the following must be recorded on F17 - Log Review Form, and KCTL [ROLE NAME] informed:

a) User Identification.
b) Event Type.
c) Date & Time.
d) Success or Failure indication.
e) Event Origination (e.g. IP address).
f) Reference to the data, system component or resource affected.

21. Secure Application development

- The Secure Application development policy is a plan of action to guide developers' decisions and actions during the software development lifecycle (SDLC) to ensure software security. This policy aims to be language and platform independent so that it is applicable across all software development projects.
- The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development on KCTL information technology systems and trusted contractor sites processing KCTL data.
- Each phase of the SDLC is mapped with security activities, as explained below:

a) Design

- Identify Design Requirements from security perspective.
- Architecture & Design Reviews
- Threat Modelling

b) Coding

- Coding Best Practices
- Perform Static Analysis

c) Testing

- Vulnerability Assessment
- Fuzzing

d) Deployment

- Server Configuration Review
- Network Configuration Review

- Development of code shall be checked and validated with the most current versions of KCTL Coding Standards for Secure Application Development. All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines.
- Only validated code shall be implemented into KCTL production environment. A review and validation ensure that code exhibits fundamental security properties to include correctness, predictability, and attack tolerance.

Application Code Developers shall:

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.
- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal etc.,), cross site request forgery (CSRF), broken authentication and session management.
- Never trust incoming data to the system, apply checks to this data.
- Never rely on the client to store sensitive data no matter how trivial.
- Disable Error messages that return any information to the user.
- Use object inheritance, encapsulation, and polymorphism wherever possible.
- Use environment variables prudently and always check boundaries and buffers.
- Applications must validate input to ensure it is well-formed and meaningful.

22. Penetration testing methodology

- In this section should be listed the risks inherent in conducting penetration testing over the information systems of KCTL. Additionally, it should be noted for each mitigation measures that will be taken. Examples might be:

Example 1#

Risk: Denial of Service in systems or network devices because of the network scans.

Mitigation measure 1: network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress.

Mitigation measure 2: scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and a use minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organization.

- Key staff involved in the project by the organization will be listed:

Technical Project Manager: George Walton
Chief Information Security Officer: George Walton
Chief Information Officer: George Walton
Head of Communications: James Cook
Responsible for web site www.kcts.me.uk: George Walton

- External intrusion tests will be performed remotely from the supplier's premises. Internal intrusion tests will be conducted in the office KCTL of the Organization. Audit team must have access to the Organization's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organization, the incident should be brought immediately to the attention of those responsible for incident management in the project.
- It should be noted that in order to comply with PCI DSS the scope of the test should include, at least the following:
    - All systems and applications that are part of the perimeter of the cardholder data environment card (CDE).

Example:

a) Systems included in the scope.

System 1: IP: System: System Description

System 2: IP: System: System Description

Wi-Fi network KCTL

.....

b) Applications included in the scope.

Application 1: URL: Description of the application

.....

c) Systems excluded from the scope.

System 5: IP: System: System Description

System 6: IP: System: System Description

.....

d) Applications excluded from the scope

Application 3: URL: Description of the application

.....

- Technical tests must follow the OSSTMM methodology. Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP and SANS, as well as those identified in the PCI DSS standard v3:

1. Injections: Code, SQL, OS commands, LDAP , XPath , etc.
2. Buffer overflows.
3. Insecure storage of cryptographic keys
4. Insecure Communications
5. Improper error handling
6. Cross -site scripting (XSS)
7. Control of inappropriate access.
8. Cross - site request forgery (CSRF).
9. Broken authentication and incorrectly session management.
10. Any other vulnerability considered High Risk by the organization.

- For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same. The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.
- As a result of tests performed should generate a document containing at least the following sections:

Introduction
Executive Summary
Methodology
Identified vulnerabilities.
Recommendations for correcting vulnerabilities
Conclusions
Evidence

23. **Incident Response Plan**

'Security incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members and take steps to ensure that they understand it and what is expected of them.

Employees of KCTL will be expected to report to the security officer for any security related issues.

KCTL PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. That member of the team receiving the report will advise the PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
5. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
6. If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Security officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
7. A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform KCTL PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

KCTL PCI Security Incident Response Team: **(Update as applicable)**

CIO
Communications Director
Compliance Officer
Counsel
Information Security Officer
Collections & Merchant Services
Risk Manager

Incident Response Notification

Escalation Members

Escalation – First Level
Information Security Officer
Controller
Executive Project Director for Credit Collections and Merchant Services Legal Counsel
Risk Manager
Director of KCTL Communications

Escalation – Second Level
KCTL Director
Executive Cabinet
Internal Audit
Auxiliary members as needed.

External Contacts (as needed)
Merchant Provider Card Brands
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Communication Carriers (local and long distance) Business Partners
Insurance Carrier
External Response Team as applicable (CERT Coordination Centre 1, etc) Law Enforcement Agencies as applicable inn local jurisdiction

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.
2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls.
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications to various card schemes

1. In the event of a suspected security breach, alert the information security officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
- Alert all affected parties and authorities such as the Barclays Bank, Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as “VISA Secret” *.

I. Executive Summary
   a. Include overview of the incident
   b. Include RISK Level (High, Medium, Low)
   c. Determine if compromise has been contained II. Background
III. Initial Analysis
IV. Investigative Procedures
   a. Include forensic tools used during investigation V. Findings
   a. Number of accounts at risk, identify those stores and compromised.
   b. Type of account information at risk
   c. Identify ALL systems analysed. Include the following:
      - Domain Name System (DNS) names
      - Internet Protocol (IP) addresses
      - Operating System (OS) version
      - Function of system(s)

d. Identify ALL compromised systems. Include the following:
    - DNS names
    - IP addresses
    - OS version
    - Function of System(s)
e. Timeframe of compromise
f. Any data exported by intruder.
g. Establish how and source of compromise.
h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
i. If applicable, review VisaNet endpoint security and determine risk.

VI. Compromised Entity Action
VII. Recommendations
VIII. Contact(s) at entity and security assessor performing investigation.

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Employees of KCTL will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within KCTL and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from Discover Card

24. Roles and Responsibilities

- Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:
- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- creating and distributing security incident response and escalation procedures that include:
- Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
- The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).
- System and Application Administrators shall:
- monitor and analyse security alerts and information and distribute to appropriate personnel.
- administer user accounts and manage authentication.
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.
- The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:
- Facilitating participation upon hire and at least annually.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand KCTL's information security policy.
- General Counsel (or equivalent) will ensure that for service providers with whom cardholder information is shared:
- Written contracts require adherence to PCI-DSS by the service provider.
- Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

25. Third party access to card holder data

- All third-party companies providing critical services to KCTL must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with KCTL's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the Card Holder data.
3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster, or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

26. User Access Management

- Access to company is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by HR/line management.
- The job function of the user decides the level of access the employee has to cardholder data
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

Name of person making request:
Job title of the newcomers and workgroup:
Start date:
Services required (default services are MS Outlook, MS Office and Internet access):

- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all company systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves KCTL employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

27. Access Control Policy

- Access Control systems are in place to protect the interests of all users of KCTL computer systems by providing a safe, secure and readily accessible environment in which to work.
- KCTL will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and

IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.

- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the KCTL
- Access to KCTL IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any KCTL IT resources and services will be provided without prior authentication and authorization of a user's KCTL Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by KCTL policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged, and IT Services shall sign off the review to give authority for users' continued access rights

28. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the KCTL networks or environments is prohibited.
- A quarterly test should be run to discover any wireless access points connected to KCTL network
- Usage of appropriate testing using tools like net stumbler, kismet etc. must be performed on a quarterly basis to ensure that:
- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology, it should be approved by KCTL and the following wireless standards have to be adhered to:

1. Default SNMP community strings and passwords, passphrases, Encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves KCTL.
2. The firmware on the wireless devices has to be updated accordingly as per vendors release schedule.
3. The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
4. Any other security related wireless vendor defaults should be changed if applicable.
5. Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of cardholder data.
6. An Inventory of authorized access points along with a business justification must be maintained. (Update Appendix B)

Part 11 SQA Streetworks - Certificate release

Certificate Processing

Keith Cook Training Ltd acknowledges SQA's policy of printing and despatching certificates directly to learner home addresses. However, to ensure quality assurances of our own systems and procedures, all certificates are returned to KCTL where they are photocopied and filed before forwarding.

At the start of each course, delegates complete a 'Confidential Delegate Information Form' to capture. Forename, Surname and home address (see attachment). Delegates are informed that the information is used solely for recording details with SQA.

On receipt of certificates from SQA, records on the SQA database are amended to record the individuals home address.

Course Booking process

On confirmation, the customer wishes to proceed, a booking form is emailed with terms and conditions here it is stated that normal costs are payable before the before the course and enables immediate release of certificates and ID cards (see attachment). Payment on account is based on 30 days from date of invoice unless otherwise agreed however, this can result in delayed release of certificates.

Individual learners

Where learners have funded their own training, and assessing, original certificates will be despatched to their home address providing.

- Payment has been received in full

Companies

Where companies are funding learners through training, and assessment, original certificates will be. despatched to the business address providing.

- Payment has been received in full

KEITH COOK TRAINING LIMITED'S GENERAL ACTION PLAN

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
Jaupt Polices & Procedure to be included within the appendices	To be completed by August 2012	31/08/2012	26/08/2013	George Walton
Jaupt Polices & Procedure to be included within the appendices amended	Completed on advice from Jaupt auditor	19/09/2012	19/09/2012	George Walton
Equality & Diversity Statement	Requires a separate statement published on notice board	12/02/2013	13/09/2013	George Walton
Whistle Blowing Policy	Adopt CT Skills	14/08/13	14/08/2013	George Walton
Matrix Re accreditation	Complete by February 2014 inspection to be completed on week commencing Monday 3rd February 2014	06/02/2014	06/02/2014	George Walton
Matrix Update	Annual Update	09/12/2014	06/12/2014	George Walton
Matrix Update	Annual Update	06/12/2015	06/02/2016	George Walton
Matrix Re accreditation	To be completed for funded provision	06/02/2017	06/02/2017	George Walton
Whistle Blowing Policy	Adopt CT Skills	14/08/13	14/08/2013	George Walton

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
First Aid at Work	To be completed December 2014	31/12/2014	22/12/2015	George Walton
Safeguarding policy introduction and course	Bruce Sheeran to complete a course for George Walton on Safeguarding, George Walton will complete and install new policy and procedure	28/02/2014	19/03/2015	George Walton
Safeguarding & prevent Training	George & Cathy to deliver	23/12/2015	23/12/2015	George Walton
Qualification Standard Setting	David to chair a standard setting day for delivery staff.	18/12/2015	18/12/2015	David Owen
LOLER Inspections	All machines that require LOLER inspections	31/05/2016	31/05/2016	George Walton
LOLER Inspections	All machines that require LOLER inspections	31/05/2017	31/05/2017	George Walton
LOLER Inspections	All machines that require LOLER inspections	31/05/2017	31/05/2017	George Walton
First Aid at Work	To be completed December 2014	31/12/2014	22/12/2015	George Walton
Safeguarding policy introduction and course	Bruce Sheeran to complete a course for George Walton on Safeguarding, George Walton will complete and install new policy and procedure	28/02/2014	19/03/2015	George Walton
CSKILLS Awards Change	All documents regarding Cskills Awards will need to be amended to reflect change of owner CITB	15/08/2017	15/08/2017	George Walton

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
LOLER Inspections	All machines that require LOLER inspections	31/05/2018	30/05/2018	George Walton
General Data Protection Regulation (GDPR)2018	Policy to be developed.	01/05/2018	18/01/2018	George Walton
LOLER Inspections	LOLER inspections Lift Apparatus only	15/12/2017	15/12/2017	George Walton
LOLER Inspections	All machines & Lifting apparatus that require LOLER inspections	31/05/2018	31/05/2018	George Walton
Matrix Telephone Audit	Matrix 1st Year Audit by Graham Walton	01/02/2018	04/02/2018	George Walton
Matrix Telephone Audit	Matrix 2nd Year Audit by Graham Walton	04/02/2019	04/02/2019	George Walton
Matrix Telephone Audit	Matrix Re Assessment Audit by Graham Walton	24/02/2020	26/02/2020	George Walton
LOLER Inspections	LOLER inspections Lift Apparatus only	15/12/2020	15/12/2020	George Walton
LOLER Inspections	All machines & Lifting apparatus that require LOLER inspections	31/05/2020	31/05/2020	George Walton
Coronavirus Policy	Create Temporary Coronavirus Policy	01/03/2020	03/03/2020	George Walton
Coronavirus Policy	Policy introduced	26/03/2020	26/03/2020	George Walton

DEFICIENCY	REMEDIAL ACTION REQUIRED	TO BE COMPLETED BY DD/MM/YY	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME
LOLER Inspections	LOLER inspections Lift Apparatus only	15/12/2020	15/12/2020	George Walton
LOLER Inspections	All machines & Lifting apparatus that require LOLER inspections	31/05/2021	30/05/2021	George Walton
LOLER Inspections	LOLER inspections Lift Apparatus only	15/12/2021	15/12/021	George Walton
Matrix Telephone Audit	Matrix 1st Year Audit by Graham Walton	24/02/2021	24/02/2021	George Walton
Matrix Telephone Audit	Matrix 2nd Year Audit by Graham Walton	24/02/2022	30/02/2022	George Walton
LOLER Inspections	All machines & Lifting apparatus that require LOLER inspections	31/05/2022	31/05/2022	James Cook
Fire Extinguisher Training	To be completed December 2022	31/12/2022	23/12/2022	George Walton
LOLER Inspections	All machines & Lifting apparatus that require LOLER inspections	31/12/2023	20/11/2023	James Cook
First Aid at Work	To be completed December 2023	31/12/2023	22/12/2023	George Walton
Fire Extinguisher Training	To be completed December 2025	31/12/2025		George Walton
Staff Overview Change		02/08/2024	02/08/2024	George Walton
Footer updated after CITB ATO EQA	Completed after CITB Audit	15/05/2025	15/05/2025	GW

DEFICIENCY	**REMEDIAL ACTION REQUIRED**	**TO BE COMPLETED BY DD/MM/YY**	DATE COMPLETED DD/MM/YY	VERIFIED BY NAME

Part 12 Additional Policies and Information for Awarding and Accrediting Bodies

CPCS Internal Quality Assurance (IQA)

KCT CPCS IQA Policy

KCT hold a centre file for IQA purposes required under the CPCS centre scheme and is held in the main office and available for review. CPCS will complete an annual EQA visit to the centre to monitor this file and processes.

KCT staff dealing with any customers CPCS requirements must follow these procedures.

1. Information Advice and guidance (IAG) must be given to customers which is current always using the CPCS documentation.
2. Follow Test centre CPCS Scheme rules for administration purposes 6.1 to 6.10 for centre administration.
3. All technical tests to be notified to CPCS at least 3 clear working days before tests are completed.
4. Advice candidates to be at the centre at least 15 minutes before scheduled test times.
5. All appropriate test documents must be ready before the commencement of tests.
6. Candidates must provide a valid ID a list can be found at 6.2 of the scheme rules, these must be original documents.
7. A CSCS Health Safety & Environmental Test must have been completed within the past two years (From test date)
8. On completion of any technical test completed documentation must be returned to the office for process
9. Completed documentation from the tester must then be signed by the receiving administration staff.
10. CPCS test results to be resulted on CPCS-ON
11. Where required a CPCS pass letter to be generated and given to candidate/tester?
12. Advise successful candidates on what happens now or
13. Advise unsuccessful candidates on what to do next.
14. All completed test documents to be secured and made available on request to a CPCS monitor for quality checking.
15. Review Risk rating for Testers based on the following criteria.

Since Last IQA (Months)	1	2	3	4	5	6	7	8	9	10	11
Likelihood of Risk since last IQA	1	2	3	4	5	6	7	8	9	10	11
Average Risk Rating level	1	2	3	4	5	6	7	8	9	10	11

Amendment History			
Version	**Date**	**Completed By**	**Policy or Procedure amended (include page number)**
1.1.3	01/03/20	George Walton	148 Temporary Coronavirus added
1.1.3	01/03/20	George Walton	66 Current Staff amended
1.1.4	03/03/20	George Walton	86 Update Fire Policy
1.1.4	03/03/20	George Walton	89 Update map
1.1.4	03/03/20	George Walton	143 Update Action plan
1.1.5	26/03/20	George Walton	COVID 19 Policy included
1.2.0	12/01/2021	George Walton	Annual Update
1.2.1	21/07/2021	George Walton	CITB SSP Audit Page 155 & 145 to include Reasonable Adjustment & Considerations
1.2.2	26/07/2021	George Walton	SQA requirements for Malpractice
1.3.0	12/01/2022	George Walton	Modern Slavery Policy introduced, and Driver CPC policies withdrawn
1.3.1	19/01/2022	George Walton	Old references to Data Protection 1998 deleted
1.3.2	26/04/2022	George Walton	Action Plan updated
1.3.4	19/10/2022	George Walton	Update ITC Policies & include into this document
1.3.5	06/01/2023	George Walton	Update ITC Policies & include into this document
1.3.6	01/07/2023	George Walton	Update ITC Policies & include into this document
1.3.7	02/08/2023	George Walton	Update to Staff
1.3.8	25/10/2023	George Walton	Update to Director & ITC IQA procedures
1.4.0	04/01/2024	George Walton	Annual Update
1.5.0	03/01/2025	George Walton	Annual Update
1.6.0	05/01/2026	George Walton	Annual Update

KCT HEALTH POLICY FOR CORONAVIRUS COVID-19 (This Policy is now for advice only)

1. Information about the virus

A coronavirus is a type of virus. As a group, coronaviruses are common across the world. COVID-19 is a new strain of coronavirus first identified in Wuhan City, China in January 2020.

The incubation period of COVID-19 is between 2 to 14 days. This means that if a person remains well 14 days after contact with someone with confirmed coronavirus, they have not been infected.

2. Signs and symptoms of COVID-19

The following symptoms may develop in the 14 days after exposure to someone who has COVID-19 infection:

- cough
- difficulty in breathing
- fever

Generally, these infections can cause more severe symptoms in people with weakened immune systems, older people, and those with long-term conditions like diabetes, cancer and chronic lung disease.

3. How COVID-19 is spread

From what we know about other coronaviruses, spread of COVID-19 is most likely to happen when there is close contact (within 2 metres or less) with an infected person. It is likely that the risk increases the longer someone has close contact with an infected person.

Respiratory secretions produced when an infected person coughs or sneezes containing the virus are most likely to be the main means of transmission.

There are 2 main routes by which people can spread COVID-19:

- infection can be spread to people who are nearby (within 2 metres) or possibly could be inhaled into the lungs.
- it is also possible that someone may become infected by touching a surface, object or the hand of an infected person that has been contaminated with respiratory secretions and then touching their own mouth, nose, or eyes (such as touching doorknob or shaking hands then touching own face)

There is currently little evidence that people who are without symptoms are infectious to others.

4. Preventing spread of infection

There is currently no vaccine to prevent COVID-19. The best way to prevent infection is to avoid being exposed to the virus.

Public Health England (PHE) recommends that the following general cold and flu precautions are taken to help prevent people from catching and spreading COVID-19:

- cover your mouth and nose with a tissue or your sleeve (not your hands) when you cough or sneeze.
- put used tissues in the bin straight away
- wash your hands with soap and water often – use hand sanitiser gel if soap and water are not available.
- try to avoid close contact with people who are unwell
- clean and disinfect frequently touched objects and surfaces
- do not touch your eyes, nose or mouth if your hands are not clean

If you are worried about symptoms, please call NHS 111. Do not go directly to your GP or other healthcare environment.

Further information is available on the PHE blog and NHS.UK.

Face masks for the general public are not recommended to protect from infection, as there is no evidence of benefit from their use outside healthcare environments.

People who have returned from Hubei Province, including Wuhan, in the last 14 days should self-isolate whether they have symptoms or not. This includes avoiding attending an education setting or work until 14 days after they leave Hubei Province.

People who have returned from Hubei Province, including Wuhan, in the last 14 days should avoid attending work. They should call NHS 111 for advice and self-isolate.

Advice is in place for what to do if you have returned in the last 14 days from specified countries or areas which is being updated on an ongoing basis.

With regards to travel information to China or other countries for individuals working in the UK, we recommend following the Foreign and Commonwealth Office (FCO) country advice pages.

At present, FCO advises against all travel to Hubei Province due to the ongoing novel COVID-19 outbreak. The FCO also advises against all but essential travel to the rest of mainland China (not including Hong Kong and Macao).

5. How long the virus can survive

How long any respiratory virus survives will depend on a number of factors, for example:

- what surface the virus is on
- whether it is exposed to sunlight
- differences in temperature and humidity
- exposure to cleaning products

Under most circumstances, the amount of infectious virus on any contaminated surfaces is likely to have decreased significantly by 72 hours.

We know that similar viruses are transferred to and by people’s hands. Therefore, regular hand hygiene and cleaning of frequently touched surfaces will help to reduce the risk of infection.

6. Guidance on facemasks

Employees are not recommended to wear facemasks (also known as surgical masks or respirators) to protect against the virus. Facemasks are only recommended to be worn by symptomatic individuals (advised by a healthcare worker) to reduce the risk of transmitting the infection to other people.

PHE recommends that the best way to reduce any risk of infection is good hygiene and avoiding direct or close contact (closer than 2 metres) with any potentially infected person.

Any member of staff who deals with members of the public from behind a full screen will be protected from airborne particles.

7. What to do if an employee or a member of the public becomes unwell and believe they have been exposed to COVID-19

If the person has not been to specified areas in the last 14 days, then normal practice should continue.

If someone becomes unwell in the workplace and has travelled to China or other affected countries, the unwell person should be removed to an area which is at least 2 metres away from other people. If possible find a room or area where they can be isolated behind a closed door, such as a staff office. If it is possible to open a window, do so for ventilation.

The individual who is unwell should call NHS 111 from their mobile, or 999 if an emergency (if they are seriously ill or injured or their life is at risk) and explain which country they have returned from in the last 14 days and outline their current symptoms.

Whilst they wait for advice from NHS 111 or an ambulance to arrive, they should remain at least 2 metres from other people. They should avoid touching people, surfaces and objects and be advised to cover their mouth and nose with a disposable tissue when they cough or sneeze and put the tissue in a bag or pocket then throw the tissue in the bin. If they don't have any tissues available, they should cough and sneeze into the crook of their elbow.

If they need to go to the bathroom whilst waiting for medical assistance, they should use a separate bathroom if available.

8. Returning from travel overseas to affected areas

People who have returned from Hubei Province, including Wuhan, in the last 14 days should avoid attending work. They should call NHS 111 for advice and self-isolate.

Advice is in place for what to do if you have returned in the last 14 days from specified countries or areas which is being updated on an ongoing basis.

All other staff should continue to attend work.

9. What to do if a member of staff or the public with suspected COVID-19 has recently been in your workplace

For contacts of a suspected case in the workplace, no restrictions or special control measures are required while laboratory test results for COVID19 are awaited. In particular, there is no need to close the workplace or send other staff home at this point. Most possible cases turn out to be negative. Therefore, until the outcome of test results is known there is no action that the workplace needs to take.

10. What to do if a member of staff or the public with confirmed COVID-19 has recently been in your workplace

Closure of the workplace is not recommended.

The management team of the office or workplace will be contacted by the PHE local Health Protection Team to discuss the case, identify people who have been in contact with them and advise on any actions or precautions that should be taken.

A risk assessment of each setting will be undertaken by the Health Protection Team with the lead responsible person. Advice on the management of staff and members of the public will be based on this assessment.

The Health Protection Team will also be in contact with the case directly to advise on isolation and identifying other contacts and will be in touch with any contacts of the case to provide them with appropriate advice.

Advice on cleaning of communal areas such as offices or toilets will be given by the Health Protection Team. and is outlined later in this document.

11. When individuals in the workplace have had contact with a confirmed case of COVID-19

If a confirmed case is identified in your workplace, the local Health Protection Team will provide the relevant staff with advice. These staff include:

- any employee in close face-to-face or touching contact
- talking with or being coughed on for any length of time while the employee was symptomatic

- anyone who has cleaned up any bodily fluids
- close friendship groups or workgroups
- any employee living in the same household as a confirmed case

Contacts are not considered cases and if they are well, they are very unlikely to have spread the infection to others:

- those who have had close contact will be asked to self-isolate at home for 14 days from the last time they had contact with the confirmed case and follow the home isolation advice sheet
- they will be actively followed up by the Health Protection Team
- if they develop new symptoms or their existing symptoms worsen within their 14-day observation period they should call NHS 111 for reassessment
- if they become unwell with cough, fever or shortness of breath they will be tested for COVID-19
- if they are unwell at any time within their 14-day observation period and they test positive for COVID-19 they will become a confirmed case and will be treated for the infection

Staff who have not had close contact with the original confirmed case do not need to take any precautions and can continue to attend work.

12. Certifying absence from work

By law, medical evidence is not required for the first 7 days of sickness. After 7 days, it is for the employer to determine what evidence they require, if any, from the employee. This does not need to be fit note (Med 3 form) issued by a GP or other doctor.

Your employee will be advised to isolate themselves and not to work in contact with other people by NHS 111 or PHE if they are a carrier of, or have been in contact with, an infectious or contagious disease, such as COVID-19.

We strongly suggest that employers use their discretion around the need for medical evidence for a period of absence where an employee is advised to self-isolate due to suspected COVID-19, in accordance with the public health advice being issued by the government.

13. Advice for staff returning from travel anywhere else in the world within the last 14 days

Currently, there are minimal cases outside the listed areas and therefore the likelihood of an individual coming into contact with a confirmed case is extremely low.

These staff can continue to attend work unless they have been informed that they have had contact with a confirmed case of COVID-19

If individuals are aware that they have had close contact with a confirmed case of COVID-19 they should contact NHS 111 for further advice.

The latest country information is available on the NaTHNac Travel Pro website.

14. Handling post, packages or food from affected areas

Employees should continue to follow existing risk assessments and safe systems of work. There is no perceived increase in risk for handling post or freight from specified areas.

15. Cleaning offices and public spaces where there are suspected or confirmed cases of COVID-19

Coronavirus symptoms are similar to a flu-like illness and include cough, fever, or shortness of breath. Once symptomatic, all surfaces that the person has come into contact with must be cleaned including:

- all surfaces and objects which are visibly contaminated with body fluids

- all potentially contaminated high-contact areas such as toilets, door handles, telephones

Public areas where a symptomatic individual has passed through and spent minimal time in (such as corridors) but which are not visibly contaminated with body fluids do not need to be specially cleaned and disinfected.

If a person becomes ill in a shared space, these should be cleaned using disposable cloths and household detergents, according to current recommended workplace legislation and practice.

16. Rubbish disposal, including tissues

All waste that has been in contact with the individual, including used tissues, and masks if used, should be put in a plastic rubbish bag and tied when full. The plastic bag should then be placed in a second bin bag and tied. It should be put in a safe place and marked for storage until the result is available. If the individual tests negative, this can be put in the normal waste.

Should the individual test positive, you will be instructed what to do with the waste.

KCT Booking Process

Each awarding or accrediting body requires specific information please refer to the booking forms for the various bodies KCT are members of which can be found on the mapped drive ‘T’ when users log in.

The following overview is a process should be followed on any communication.

1. Establish who you are communicating with, including company.
2. Offer information, advice and guidance on the various options available to the customer making sure not to make any personal recommendations.
3. Once the training requirements have been established refer to the company diary for availability, explain the dates are not on hold at this point but if they would like to go ahead and book them the dates will be held for 3 working days.
4. To make a booking you will require a contact number and email to send the booking form/s to enter these details into the diary so that if you are not available another staff member can interact with the customer.
5. Confirm all pricing which can be found from the pricing documents on the Mapped drive ‘A’
6. On receiving booking forms, print them off and amend the diary accordingly, the forms must be given to accounts for processing.
7. Once the diary and forms are in place reply to the customer thanking them for their business and confirming their dates are now confirmed.

KCT IQA PROCESSING

Principals of an IQA

Ethical conduct:
Trust, integrity, confidentiality, and discretion are essential to auditing.

Fair presentation:
Audit findings, conclusions and reports reflect truthfully and accurately the audit activities.

Professional care:
Auditors must exercise care in accordance with the importance of the task they perform.

Independence:
Auditors must be independent of the activity being audited and be objective.

Evidence-based approach:
Evidence must be verifiable and be based on samples of the information available.

KCT INTERNAL AUDIT FORM

What Is an Internal Audit Form?

An Internal Audit Form is an audit report form that compiles all the data and information about a particular organization's quality of performance during a specific period. It displays and summarizes each of its parts', workforce, and equipment alike, performance with statistical data. This report also serves as a review from which plans will be drawn from. An Internal Audit Form also serves as a platform for improving and calibrating the whole organization's performance.

The Report Form

KCT have produced an internal quality audit form to cover all deliveries of staff. This form (included in this process document) includes the full process which must be completed fully and if any areas are not applicable a line must be put through that section, the last page can be extended to allow the auditor and delegate to expand on feedback or action points.

Both parties must agree with the content by signing and dating the footer of this document.

At no time should the IQA consult with the instructor/tutor in front of any delegate/s on the course, any feedback should be given outside of the course delivery, this would lead to undermining the instructor/assessor.

The IQA is to maintain standards set by the awarding or accrediting body (AOs), these reports can be requested by the AOs at any EQA visit to the centre. KCT IQA is now recognised by one AO in particular The Association of Industrial Truck Trainers (AITT) and is now a requirement if training providers want to achieve their certificate of excellence.

Purpose of this process

To meet and exceed the requirements placed upon us by.

Our accrediting bodies.
Other awarding bodies.
Our delegates.

To support all employees to have excellent working practices, through provision of formative training, supervision, observation and sampling processes.

To support and develop tutors in their working practices by affording them the opportunity to receive critically supportive comment on;

The assessment decisions reached on portfolio evidence
Training/teaching techniques applied To ensure provision of secure, hospitable, inspiring and engaging settings for learners.

To provide a continuous check on the consistency and quality of delivery and the consistency, quality

and fairness of marking, grading and overall assessment of learner evidence. To ensure that valid, consistent assessment decisions are reached, and external requirements are fully met.

To develop and maintain internal and external associations based on quality, belief and integrity. And so to encourage and uphold quality in all that we do.

Scope

All employees, tutors, and delegates; Internal Quality Assurance of any work practices, documents and evidence that impact on the delivery, examination and assessment of qualifications and training supplied by the Training Centre. C) Roles and Responsibilities
Our manager is responsible for ensuring that.

The quality requirements of our accrediting university, other awarding bodies and employment partners are met in the delivery and assessment of qualifications.

IQA policies and procedures are sufficient, regularly reviewed and known, understood and implemented by all.

All employees and tutors involved in the processes of delivery of services are appropriately. trained and qualified through provision of rigorous recruitment processes, induction training. and continual development.

All employees and tutors involved in IQA processes are appropriately trained and qualified. through provision of rigorous recruitment processes, induction training and continual development. Employees and tutors involved in induction of Delegate/s are responsible for ensuring:

Checking the identity of the Delegate/s;

All paperwork is fully and accurately completed.
That Delegate/s are inducted into their chosen programme in a way that meets their needs. Tutors are responsible for ensuring that:

Candidates/learners are aware of.
The different types of evidence that they can collect to prove competence of knowledge and working practices.
Their responsibilities in the collection, authentication and presentation of evidence.

The candidates/learners are fully supported throughout the term of their qualification. This should include:
Assessing the persons learning style and discussing their preferred ways of learning
Effective management evidence gathering, assessment and attainment.
Agreeing and recording assessment and visit plans for each person.
Completing regular reviews with the person and their employer to review progress. and agree new targets.
Providing the person with prompt, accurate, formative and summative feedback.
Demonstration of anti-discriminatory practice and equal opportunities
Maintenance of confidentiality and compliance with the Data Protection Act.

They observe learners' performance through formative assessment and/or in simulated. situations, and/or conduct other forms of assessment in accordance with the qualification and unit standards and requirements of the QCF and the accrediting university. Such as; ensuring validity, authenticity, currency and sufficiency of evidence maintaining appropriate, accurate and verifiable records confirming that learners have demonstrated competence/knowledge and have completed the required documentation.
As required, they make themselves available and organise for their Delegate/s to be available to the Manager and external Quality Assurers from our accrediting university and other awarding bodies.

Internal Quality Assurers

Internal Quality assurers are responsible for:
Ensuring that they lead, advise and support the tutors allocated to them through;
Ensuring adherence to the principles of assessment and guidance provided by the centre;

Providing guidance on the interpretation and application of assessment criteria correctly and consistently applied;

Observation and supply of formative feedback on working practices;
Sampling of assessment activities such as assessment decisions, formative feedback supplied, completion of portfolio documents, Delegate/s evaluation forms, etc;
Ensuring assessors have opportunities for updating and developing their vocational and professional competence;
Carrying out a quality audit of the documentation used within and format of the training courses;

Supporting, countersigning, dating assessments and quality assuring judgements by assessors and Internal Quality Assurers not holding the appropriate assessor/Internal Quality Assurer qualifications as approved and specified by the Regulatory Authorities.

Supporting the Training Centre to meet its goals by;

Undertaking an active role in raising issues of good practice in assessment;
Ensuring that equal opportunities and anti-discriminatory practices are upheld in the assessment process;
Liaising with other IQAs and the External Quality Assurer to implement the requirements of the assessment system;
Ensuring that all Learners' achievement records and Centre documentation are completed in accordance with requirements; Attending regular IQA meetings.

Policy Implementation – Procedures
The IQA policy must be applied to every programme with work that is internally assessed and which contributes to the final assessment outcome of a Delegate/s. Tutors and Internal Quality Assurers will be given sufficient time, resources and authority to perform their roles and responsibilities effectively.

Qualifications Only appropriately qualified and experienced tutors must carry out un-supported assessment. All
tutors must have significant experience in the sector of the qualification Appropriately qualified staff must carry out all internal quality assurance.

Sampling All IQAs must follow the sampling plan developed and maintained by the Manager. Sampling must be across all tutors, all types of evidence and all Delegate/s, including plans, reviews and records in addition to Delegate/s evidence.

Frequency of assessment will be decided following a risk assessment of the assessor, looking at experience and competence, but to meet the requirements of the accrediting university, other awarding bodies and our partners all portfolios will be quality assured the IQA will at the minimum.

sample at least one piece of evidence for each component of the qualification. IQA must be carried out continuously throughout the year.

Observations

All tutors will have at least one observation per year by their allocated IQA. IQA observation should include.
Sight of Learning Plan
Agreement of objectives for the meeting/visit/session
Delegate/s performance and stretching.
Embedding of Functional Skills, Safeguarding and Equality & Diversity
Questioning / Assessment / Training / Self-guided learning
Formative feedback
Recap of learning achieved.
Agreement of next steps

The observation will be recorded on an Observation of Assessor Practice Form. Feedback from an IQA observation of trainer delivery must be delivered to the relevant trainer as soon as practicable, preferably by the end of the working day. Any actions should then be agreed, and the Observation of Tutor Practice form should be updated and then signed by the IQA and tutor to confirm the accuracy of the information it contains. A copy of the form should be forwarded to the Manager and the original filed in the tutor's personnel file.

Delegate/s Interviews

Once a year the IQA will interview at least one Delegate/s for each of their allocated tutors. There are set interview questions on the Learner Interview Record, all of which should be asked, but all may not be applicable. These interviews may be carried out face to face or by email. Once complete a copy of the record should be forwarded to the Manager and the original filed in the tutor's personnel file.

Disagreement of IQA findings

Every tutor has the right to challenge an IQA decision made on their assessment decisions. The assessor should indicate their disagreement on the relevant IQA form and bring it to the attention of the IQA within 5 working days of being informed that the portfolio is ready for collection following an IQA. Where there is a challenge made the assessor and IQA must in the first instance meet and discuss the challenge informally, if agreement can then be made, this should be indicated on the IQA form and then no further action is required. If an agreement cannot be reached, then this goes to:

Stage One Appeal

The lead IV will allocate another IQA to investigate the challenge.
They will discuss the IQA report with the assessor and the first IQA and will IQA the piece of evidence/document
themselves and will inform the Lead IV and centre manager of the results of their investigation.

The Lead IV or centre Manager will inform both parties of the result.

That decision can be appealed by either party and will then go to:

Stage 2 Appeal

The Lead IV will listen to all parties, review the evidence and will rule on evidence/document.
The lead IVs decision is final.

Standardisation & Development

The Training Centre will host at least four team development meetings every year. These meetings will normally be held at the same time and include a general team meeting. These meetings are also used to discuss any updates from the accrediting university, other awarding body, QCF and partners to ensure understanding and consistency of delivery and supply assessors and IQAs with packs of information on the same.

Tutor development & standardisations will be recorded in the meetings minutes and all tutors must update their CPD with details of development. All tutors are encouraged to continually develop their skills and knowledge in their assessment sectors and in teaching and training techniques.

IQA Team Meetings

All Internal Quality Assurers must attend annual IQA meetings chaired by the Manager. These meetings are used to discuss:
Any new standards;
Any new accrediting university or awarding body guidance;
Required standardisations;
Any issues since the last meeting;
Expected standards.

TRAINING AUDIT VISIT TO INSTRUCTOR/ASSESSOR/STAFF

General Information	Comments
Monitor Name	
Instructor/Assessor/Staff Name	
Employer	
Was the visit pre-announced?	YES/NO
Venue	
Course Title	
Course Code	

Organisation & Preparation			
Did the site provide the following	**Yes**	**No**	**Comments**
HSE compliant machinery			
Suitable Site			
Suitable Site Facilities			
Suitable Equipment			
Provide correct course deliverables (skills guides/workbooks/supporting literature			
Allow only suitable delegates to attend the course			
Take account of delegate ratios (to include social distancing)			
Ensure all requirements as per course portfolio sheets are met			
Provide Application forms and ITA assessment paperwork			

Scale: 1 = Very Poor 2 = Poor 3 = Satisfactory 4 = Good 5 = Excellent

Organisation & Preparation	Rate	Comments
Use Of site specific and generic risk assessment		
Presentation and Instructional Techniques		
Highlighting of course/session aims and objectives		
Coverage of the health and safety issues relating to course/task		
Use of facilities and equipment		
Use of course/task related documentation		
Rapport with delegates including encouraging discussion/questions		
Explanation and demonstration		
Structure of course/session		
Use of constructive & encouraging error correction techniques		
Questioning of delegates to check understanding/past experience		
Technical standards		
Level of subject knowledge		
Credibility with delegates during course/session		
Level of health and safety knowledge displayed during the course/session		
Assessment (ITA only)		
Briefing of delegates on the assessment procedure		
Delivery of the assessment task/activity		
Completion of the documentation and feedback given		

Comments and recommendations for instructor/assessor		
	Comments/recommendations	By when
Organisation and preparation (within the		

instructors control)		
Presentation and instructional techniques		
Technical standards		
Assessment (ITA only)		
Other		
Comments and recommendations for provider		
Organisation and preparation		
Course requirements as product portfolio sheet (i.e. venue, site equipment, etc)		
Other		

Company Vehicle Incident Procedures

This procedure must be followed by all staff using company vehicles on the highway.

If an incident happens and you are physically able, you must complete this procedure whilst maintaining your own safety. DO NOT put yourself in a unsafe situation.

Once you are in a safe situation complete the following procedure:

Accidents

Should a driver of a Company vehicle be engaged in any road traffic accident, they must do the following:

- Immediately after a road traffic accident involving a company vehicle.
- Call the police on 999 only if there are injuries or the road is blocked.
- However, minor you think the accident is, YOU MUST STOP. Failure to do so is an offence under the Road Traffic Act.

- You should make sure your vehicle's engine is switched off and then turn your hazard lights on to alert other road users to your presence.

- Take a look around and if anyone has been injured in the accident, you should call the police (and an ambulance, if necessary) as soon as possible.

Giving details after a road traffic accident

When you're involved in a road traffic accident, you're obliged to give your name and address to anyone else involved.

However, you should avoid saying accepting blame for the accident until you know precisely what happened, as it could be held against you later.

You should stop and give your details if you crash into something on or near the road, even if there aren't any other people involved. If you hit a parked car, for example, you should leave your details on the windscreen.

Collecting details after a road traffic accident

After an accident, collect as many details as possible. If possible, you should collect the following information from any drivers, passengers and witnesses:

• Names

• Addresses

• Contact numbers.

Ask the other drivers involved for their car insurance details, and try to establish whether they are the registered keeper of their vehicle. If they are not, find out who is and make a note of their name and address.

Call the police straight away if someone leaves the scene of the accident without giving their details.

Other information to collect from the scene of the accident

Here are some other important details you should try to collect at the scene of the accident:

• The registration numbers of all vehicles involved, plus a note of each vehicle's colour, make and model

• The time and date of the accident

• A sketch showing the positions of vehicles involved

• A description of the weather conditions, plus anything unusual you notice about the road quality or lighting

• The names of any witnesses or police officers at the scene

• A list of damage to vehicles, and a description of any injuries sustained by pedestrians, drivers and passengers.

If possible, take some pictures at the scene of the accident for use as evidence.

Report immediately to KCT Main office Once you have gathered all information you must immediately contact the main office to report the accident and, if the vehicle was damaged and cannot be driven, to arrange for it to be taken to a repair centre.

INFECTIOUS DISEASE OR VIRUS PANDEMIC

Purpose of the policy:
Keith Cook Limited strives to provide a safe and healthy workplace for all their employees, trainees and contractors. This infectious disease or virus pandemic policy outlines our overall response to a pandemic outbreak and our emergency preparedness and business continuity plan. It outlines specific steps Keith Cook Limited will take to safeguard employees', trainees and contractor's health and well-being during a pandemic while ensuring Keith Cook Limited ability to maintain essential operations and continue providing essential services to our customers. In addition, it provides guidance on how we intend to respond to specific operational and human resource issues in the event of a pandemic.

Pandemic defined:

Pandemics can occur when mutating viruses become transmissible to humans, who generally lack any natural immunity to fight off the viruses' adverse health effects. Because infected humans are so contagious, they become the primary vehicle for pandemic spread. The more humans who become contagious, the more widespread the disease becomes and the more rapid the spread is. Generally, pandemic occurs in waves, with each new group of infected people in turn infecting others. Each such wave of infection can last for a long period, resulting in steadily increasing numbers of infections, until it has run its course through the population.

Pandemics pose a serious global threat to public health and our economy. It conceivably can cost billions of pounds in productivity losses resulting from absenteeism, pay out of sick leave or workers' compensation, and lost venue; disrupt transportation and communication services on which we all depend; and impede delivery of necessary goods and services. Inability to predict when such a disease might strike and with what severity makes it incumbent on Keith Cook Limited to consider how our business might be affected and to articulate what needs to be done to respond to an outbreak.

Identification of essential personnel:

Keith Cook Limited will identify employees designated as essential personnel whose jobs are vitally important to our continued operation in emergencies. We expect only designated essential personnel to be available for work during any pandemic. We acknowledge, however, that even essential personnel might become ill and unavailable to work or not be able to reach our workplace because of conditions beyond their own or our control. Consequently, Keith Cook Limited will equip our most essential personnel with all the resources, including computers, mobile phones, and printers, that essential employees may need to work remotely during emergencies.

Infection-control measures:

Keith Cook Limited will take steps to minimize the extent as far as practicable to the exposure and spread of infection in the workplace, which is an ideal site for contagion because of workers could be working in proximity to one another. As appropriate, Keith Cook Limited will enforce all recommended measures from the Government and the UK Health Security Agency to ensure employees can protect themselves both inside and outside the workplace.

Ill employees:

Keith Cook Limited expects employees who contract the illness or have been exposed to infected family members or others with whom employees have been in contact with to stay home and seek medical attention as necessary and appropriate. Keith Cook Limited expects such workers to notify us as soon as possible of exposure or illness to enable any specific actions to be taken to protect other workers.

In the event of a pandemic Keith Cook Limited will ask all employees to complete a course risk assessment to include any illness that will reflect Government and UK Health and Security Agency guidance to ensure they are safe to be at work. On arrival to work all employees, trainees and contractors will complete and sign a site

specific risk assessment that will cover infectious disease or virus pandemic daily signing in and out register and statement of fitness to work.

Personal protective equipment:

Keith Cook Limited will maintain suitable and adequate supplies of recommended personal-protection equipment, such as face masks, eye protection, rubber gloves, and anti-bacterial hand gels and wipes that Keith Cook Limited will require workers to use.

Business travel:

Keith Cook Limited will make all reasonable efforts to eliminate the need for travel by taking advantage of technology that allows us to communicate or otherwise operate electronically. Generally, in the event of a pandemic, travel on Keith Cook Limited behalf would be suspended and limited to a select group of essential personnel who have obtained required travel authorizations from Keith Cook Limited to ensure they have social distancing. Vehicles touch areas such as: door handles, steering wheel etc. will be regularly sanitized. When feasible employees may use their own vehicles to travel to and from home to ensure safe distancing.

Site cleaning:

In the event of a pandemic there is added responsibility on all employees to keep themselves clean along with the workplace and welfare facilities. Keith Cook Limited will ensure that all welfare facilities are regularly cleaned and sanitized throughout the working day.

Site procedures and assessment:

Prior to any work being carried out away from the centre a risk assessment will be carried that will consider:

- Workers suitability to work
- Travelling to and from work
- Location access and egress
- Hand washing facilities
- Toilet facilities
- Canteen and rest areas
- Changing facilities if required
- Cleaning
- Emergency first aid

Accommodation:

Whilst working away there may be a need for accommodation and Keith Cook Limited will ensure there is social distancing that will require separate rooms for each person.

In some cases, the Government may close down all accommodation and in these cases if it is not viable to travel daily the work will be suspended.

Return to work from holiday.

To ensure the risk of any viruses spreading through the workforce all employees will communicate with KCTL main office staff stating if they have been anywhere where they will have to self-isolate on return from holiday.

If they have to self-isolating, they must have approval from the main office to return to work on completion of their isolation.

KEITH COOK CITB ITC & SSP POLICY & PROCEDURES

(Additional information included from main policies for ITC & SSP included in this section)

CITB ITC & SSP Chart

Position	Name
Chief Administrator for CITB ITC	Janet O'Keeffe
ITC Manager	George Walton
Administrators for ITC	Janet O'Keeffe/James Cook/George Walton
IQAs for ITC	Janet O'Keeffe/James Cook/George Walton
CITB Site Safe Plus Chief Tutor	David Harding
IQAs For CITB SSP	Janet O'Keeffe/James Cook/George Walton
Exam CITB SSP Verbal Delivery Support	Janet O'Keeffe & George Walton
Exam CITB SSP Verbal Delivery Support IQA	David Harding

ITC General requirements and procedures for booking tests

To verify a candidate's username, contact the CITB test provider on 0800 145 6084, (UK office hours only).

Keith Cook Training Ltd (The ITC) shall put in place and maintain a system enabling prospective Candidates to book and pay for a Test to be taken at the Test Centre, which system shall comply with the following:

Where payment by debit or credit card is accepted, the ITC's system shall be PCI compliant at all times and in all respects.

The following information will be collected in respect of every Candidate (this information will be required when booking the Test with Pearson VUE):

- Candidate's full name
- Candidate's full address including full postcode;
- Candidate's nationality;
- Candidate's contact numbers;
- Candidate's email address (if available);
- Candidate's CITB registration number (if available);
- Candidate's National Insurance number;
- type of Test booked;
- any Additional Candidate Support required such as a voiceover or BSL; and
- such other information as CITB may from time to time require the ITC to collect on arranging a booking for a Test.

The ITC shall enter into a contract with all Candidates which includes as a minimum the provisions set out in the CITB Testing Services Internet Test Centre (ITC) Information Pack with candidate test booking confirmation kept on record for 2 years.

When booking Tests on behalf of a Candidate, the ITC shall follow the booking procedure set out. All bookings made by the ITC on behalf of any Candidate shall be subject to the CITB Terms and Conditions as set out on the Pearson VUE booking system, including, for the avoidance of doubt, the terms and conditions relating to rescheduling and cancellation.

The candidate must be given a copy of the Candidate Rules Agreement to read prior to signing the electronic e- pad and to sitting the test, see CITB Testing Services Internet Test Centre (ITC) Information Pack.

Approved ITCs are granted the right to book and deliver Tests to Candidates at the Test Centre, including taking booking requests from prospective Candidates and booking Tests through the Pearson VUE booking systems, subject always to the terms and conditions set out in the Agreement, fulfilment of application criteria, related policies, and Technical Requirements.

For the avoidance of doubt, in arranging bookings for Tests or other activities undertaken by the ITC, including but not limited to, supplying CITB products, the ITC shall operate at all times as an independent contractor, and shall not act, and shall not represent itself to Candidates as acting, as an agent for or otherwise on behalf of CITB.

Any waiver forms or parental consent forms must be retained, electronic signatures taken and checked

against the identification provided. (How to book a candidate in for their test can be found within the ITC Policies and Procedures which you should retain a copy of and can be found at http://www.citb.co.uk/about-us/how-we-work/policiesguidelines/

If the signature does not match the identification provided, the candidate has another chance to electronically sign. If this is again incorrect, the candidate must be refused a test.

Images of the candidates must be taken to the correct standard (which can be found in Appendix 13 to this document), however this should be of the candidate's head and shoulders, clear, with the

candidate looking at the camera, eyes open, against a neutral background, with no obstructions in the background. If the initial photograph is not of the required standard, this will need to be re-taken again).

Prior to admitting any Candidate to the Test Room, the ITC shall ensure that the following is completed by either the Chief Administrator or the Test Administrator:

CITB Testing Services

Inspect and take a copy of the Candidate's current valid passport, photo driving licence or other appropriate form of identity as set out in Appendix 5 and retain them securely for two years.

Take a photograph of the Candidate using the methods set out in the Application Form;

Require the Candidate to sign the Test Log to confirm the time of the Test and consent to having their image taken.

Require the Candidate to sign the electronic signature pad to confirm that they have read the following, in hard copy format at booking in stage as per ITC Policies and Procedures:

The Candidate Rules Agreement and a Fire Safety Briefing giving details of evacuation procedures and meeting points in the event of emergency.

Check that the signature on the electronic signature pad matches the signature on the ID presented by the Candidate and any Candidate who is unable or unwilling to provide the above shall not be admitted to the Test Room.

Pricing of tests

The price charged by the ITC to Candidates for each Test shall not exceed the relevant Test Fee set on the CITB website (as varied by CITB from time to time). The ITC shall be responsible for collecting the relevant Test Fee(s)
from Candidates.

In the event that the ITC provides Tests as part of a wider service offered to Candidates, it shall ensure that the Test Fee is clearly stated separately from all other fees or charges applied.

Data protection

Notwithstanding the Agreement and for the avoidance of doubt, the ITC shall retain Candidate Data in a secure and locked place for two years from the date of its collection and ensure that all Candidate Data is disposed of in a secure
manner fully in accordance with the DPA.

Administration of bookings

The administrators are responsible for all KCT test bookings made by the ITC.

Registering and booking Candidates for tests

It is the responsibility of the chief administrator to ensure that candidates are made aware of the date and time of their test booking. Candidates must be informed of the types of identification that are acceptable. A list of acceptable documents is shown in Appendix 5 to this document. Candidates must be warned that they will not be able to test if they do not present appropriate identification on arrival at the ITC.

If a candidate does not have appropriate identification, a waiver form, together with a letter giving guidance for completion, (Appendix 6 and Appendix 7 to this document) can be offered to the candidate for completion prior to the test date. The form must be fully and correctly completed, with all required documents attached, when offered as identification for a test. If the form has not been completed correctly the candidate must be refused a test. These must also be kept on site for audit purposes for two years.

Waiver forms are available on the download section on the Pearson VUE VSS website or at www.citb.co.uk/testing services. These should only be used in exceptional circumstances when a candidate has no other form of identification from the requested ID list, Appendix 5. For clarity, no ITC is allowed to confirm identification of a candidate who is testing at the same ITC.

It is recommended that all candidates taking the HS&E test view the Setting out film, which is available for download free on the website www.citb.co.uk/settingout.

It is also recommended that candidates thoroughly revise and prepare before taking their HS&E test. The best way of doing this is to use the official revision material which is available to purchase from www.citb.co.uk/hsanderevision, (see section 23 of this document).

Registering and booking Candidates under the age of 16

In order to book an under-16 candidate for a test, please contact the Pearson VUE helpline on 0161 855 7459.

CITB must have proof of parental permission to register and hold a record for persons under the age of 16. Parental consent must be obtained to register a person under the age of 16. The parent (or guardian) must be given a parental consent form to complete see Appendix 8 to this document. No candidate under 16 is allowed to test under the CITB ITC agreement without first having obtained parental permission to do so. A parent or guardian must also accompany an under 16 candidates to their test.

It is the ITC's responsibility to ensure that all required documents detailing parental / guardian authorisation are both requested and received by the ITC prior to any candidate under the age of 16 commencing a test.

In exceptional circumstances, where the candidate is under the age of 16 and does not have any form of photographic identification (for example a passport), they can present the Under 16 confirmation of ID form see Appendix 9 to this document. This form must be signed by the college or school at which the candidate attends.

The test administrator(s) invigilating the test cannot sign this form on behalf of a candidate.

Both forms are available from the download section of the VSS website, or at www.citb.co.uk/testingservices.

The ITC must securely store the signed parental consent form and under 16 confirmation of identification form on site for audit purposes, for two years.

ITC staff

The ITC shall appoint an Administrator who shall:

Give such assistance as may be necessary to any CITB representative carrying out Quality Assurance monitoring at the ITC;
Monitor and maintain the security, both physical and on-line, of the Test Room and equipment;
Monitor conditions in the Test Room and ensure compliance with this Agreement;
Book and confirm times of Tests with Candidates, as per ITC Policies and Procedures and communicate any re-schedules or cancellations to the Candidates;
Ensure that every Candidate sits the type of Test which they booked;

The ITC shall:

Notify CITB of the identity of its Administrator at the Commencement Date and shall notify CITB as soon as reasonably practicable of the identity of any new Chief Administrator appointed.
Ensure that any individual which it intends to act as a Test Administrator shall have successfully completed the test

Administrator Training and passed the ITC Administrator Test and is retaken every 12 months.
Ensure that, at all times during a Test, Test Administrators are present, within the Test Room in a ratio of at least one to every eight Candidates present.

Be sufficiently resourced to make sure that invigilation and administration tasks are carried out in line with the Scheme Rules.

Procure that the Test Administrator complies at all times and in all respects with Pearson VUE's rules and procedures as issued to Test Administrators or published within the VUE Support Service from time to time.

The Test Administrator, the ITC, the Company Administrator, and other Test Centre representatives must demonstrate sufficient English language competency to be able to act as scribe or reader for (a) Candidate(s), as and when needed, and to make intelligible announcements during the Test.

Administrative requirements
Test Logs in respect of each Test taken at the Test Centre to be completed fully and accurately and securely kept on file at the Test Centre premises for 2 years from the date of the Test to which they relate. After 2 years, test logs will dispose of using a cross shredder.

The Test Administrator/ invigilator is responsible and accountable for the following:

Booking Candidates in 48 hours before their HS&E test. CITB will waive this rule only in exceptional circumstances.

Making sure that every Candidate sits the type of Test that they have booked.

Ensuring compliance in all respects with CITB and Pearson VUE rules and procedures, as issued to Test Administrators or published on the Pearson VUE Support Service (VSS) from time to time.

Making sure that each Candidate Test start and finish time is recorded according to the actual Candidate Test time on the Test Logs.

Making sure that, once a Candidate leaves the Test Room after completing the Test, the leaving time is logged.

Being present in the Test Room to make sure that the Tests are correctly invigilated while a Test is in progress. For the avoidance of doubt, the Test Administrator must always be physically present in the Test Room during the entire testing process. The use of viewing windows or CCTV Test monitoring is not

permitted. Without exception, the Test Administrator must not have a mobile phone or any personal electronic device in the Test Room or on their person during the testing process.

Keeping secure and not sharing their Test Administrator login details or password with anyone and not allowing any other person to use their login details or password.

Internal Quality Audits (IQAs) are to be completed 4 times per year and reports filed behind the log sheets relevant to the time and date of the tests being audits. These audits will be completed retrospectively to avoid any unnecessary distractions to delegates completing their testing. It will also avoid any excuse to use by delegates for complaints.

Reasonable Adjustments Policy

UK Government Guide

1. What we mean by reasonable adjustments

Under the Equality Act 2010 public sector organisations have to make changes in their approach or provision to ensure that services are accessible to disabled people as well as everybody else. Reasonable adjustments can mean alterations to buildings by providing lifts, wide doors, ramps and tactile signage, but may also mean changes to policies, procedures and staff training to ensure that services work equally well for people with learning disabilities.

For example, people with learning disabilities may require :

- clear, simple and possibly repeated explanations of what's happening and of treatments
- help with appointments
- help with managing issues of consent in line with the Mental Capacity Act.

Public sector organisations shouldn't simply wait and respond to difficulties as they emerge: the duty on them is 'anticipatory', meaning they have to think out what's likely to be needed in advance.

All organisations that provide NHS or adult social care must follow the accessible information standard by law. The standard aims to make sure that people who have a disability, impairment or sensory loss are provided with information that they can easily read or understand with support so they can communicate effectively with health and social care services.

2. What we mean by learning disabilities

A person with learning disabilities will have:

- a significantly reduced ability to understand new or complex information and to learn new skills, this is known as impaired intelligence
- a reduced ability to cope independently, this is known as impaired social functioning

These will have started before adulthood, with a lasting effect on development.

This doesn't include conditions like dyslexia, which cause a specific difficulty with one type of skill but not a wider intellectual impairment.

Public Health England (PHE) estimates that 1,087,100 people with learning disabilities, including 930,400 adults, were living in England in 2015. The number of people with learning disabilities recorded in health and welfare systems is much lower. For example, GPs identified 252,446 children and adults as having learning disabilities on their practice-based registers. Those on the registers are likely to be people with more significant learning disabilities.

3. What you might notice if someone has learning disabilities

Some people with learning disabilities look a little different – for example, a member of a health care team might notice a person with Down syndrome – but lots of people do not. It will usually be relatively easy to identify someone with more significant learning disabilities and information may well be passed on by the GP, family carers or support staff. Health teams need to be alert to the larger number of people with mild learning disabilities, who may still need some support.

You might notice someone who has difficulty with:

- reading or writing and forms
- explaining symptoms or a sequence of events
- understanding new information or taking information in quickly
- remembering basic information such as date of birth, address, health problems
- managing money
- understanding and telling time

If you notice someone with these difficulties, you should speak to them to ask more questions about their communication or support needs and check if they understand and remember information.

4. Keith Cook Training Delivery

The UK Government guide above is to be used to help Keith Cook Training staff to support delegates meeting the training standards set by the accrediting or awarding organisations. We cannot work outside of these bodies standards.

CITB Site Safety Plus Quality assurance requirements

Delegates with special assessment requirements can request the assistance of the invigilator, if required. Discussions to accommodate delegates with special requirements should be arranged prior to the course and separate arrangements must be put in place.

Prior to course commencement, Training Providers should identify any special requirements that delegates may have, such as physical disabilities, including sight, hearing or writing, and learning or reading difficulties (for example, dyslexia). It is important to remember that sensitive information about the delegate has been offered voluntarily and it should be respected as confidential and in accordance with data protection and equality legislation.

In circumstances where assistance is required, the training Provider should know that under the Equality Act 2010, the training Provider is specifically required to make ‘reasonable adjustments’ or give ‘special consideration’ to enable everyone to have an equal opportunity to complete the course.

You must also be mindful not to make the course easier or for any individual to gain an advantage through any special considerations or reasonable adjustments that you apply. The integrity of the examination must not be compromised.

You must discuss with the delegate what support they need and be prepared to arrange for adaptations (for example, the examination can be held in a separate room and questions can be read to the delegate), which may include additional staff support.

Malpractice & Maladministration Policy – The following information wording is specific to CITB and is in addition to the main policy.

Malpractice is a deliberate, reckless (intended or unintended) act of an individual or business to dishonestly claim certificates for delegates, or to obtain such achievements through fraud or deception. Furthermore, malpractice is an act that does not comply with the requirements of CITB and brings the authenticity, reliability and integrity of a CITB training qualification into question.

KCT will review at least annually, arrangements for preventing and investigating malpractice and maladministration through your QMS, policies, procedures, and staff training, which include how you will deal with and report all such occurrences.

KCT will report all cases of alleged and proven malpractice, that are identified, by email to CITB at report.it@citb.co.uk

All staff, including contracted trainers, must have detailed knowledge of KCT training organisation's malpractice, maladministration, counter fraud and whistle-blowing policies. These policies and procedures are available to all staff on a shared drive and can also be downloaded from www.kcts.me.uk

All KCT ITC/SSP paperwork to be stored and accessible for a period of three years.

Further information for Quality assurance from CITB can be found at their website.

Conflicts of interest – The following information wording is specific to CITB and is in addition to the main policy.

KCT will maintain an up-to-date conflict of interest policy and a log that details the conflict and mitigation taken to manage conflicts.

A conflict or perceived conflict can be defined as a situation in which a person has a private or personal interest, sufficient to appear to influence the objective exercise of his or her official duties as, for example, a trainer's family member or a company employee. CITB Invigilator test can be complete at the centre

Trainers who work for more than one training Provider must declare this information to any new or existing training Provider they work for.

Details of any conflict of interest must be recorded on the training Provider's conflict of interest log and be made available to the Senior Quality Consultant for audit on intervention visits.

Conflicts of Interest Declaration Form

Introduction

This Declaration Form is intended to capture conflicts of interest relating to individuals involved in the aforementioned CITB SSP/ITC policies to avoid any distortion and to ensure equal treatment.

Involvement, in the context of conflicts of interest, may relate to any stage in the commercial lifecycle including preparation and planning, publication, selection and award and contract implementation.

Individuals must avoid placing themselves in a position where there is a conflict between their personal and/or outside interest and their official duties and must comply with internal policy relating to gifts, hospitality and conflicts of interest at all times.

Examples of conflicts of interest may include, but are not restricted to:

- if you are a current or previous employee of a company, or have a member of your family, your partner (married, civil partnership or not), your siblings, your children, or any close personal or professional relationships that are an employee of a company, that is seeking to do business with the Contracting Authority;
- if you, or a member of your family/friends (as set out above), has a financial interest in a company that is seeking to do business with the Contracting Authority;
- if you, or a member of your family/friends (as set out above), has a financial relationship of any kind with a company seeking to do business with a Contracting Authority.

This is a non-exhaustive list of examples and it is your responsibility to ensure that any and all actual, potential or perceived conflicts are disclosed prior to you being involved in the procurement.

If you are unsure whether your current or previous relationship or involvement with a company that is seeking to do business with the Contracting Authority constitutes a conflict of interest, you should seek advice from an Authorised Individual stated below.

This Form also includes a requirement for individuals involved in the procurement to treat information (including but not restricted to bid documents, supplier evaluations etc.) with the appropriate level of confidentiality, and not make any unauthorised disclosures of this information.

All individuals involved in any conflict of interest must sign this Form.

Authorised Individuals

Authorised Individuals are responsible for managing the disclosure of procurement information and conflicts of interest. The Authorised Individuals for KCTL:

James Cook MD

George Walton

Janet O'Keeffe

If conflicts of interest arise at any time, an Authorised Individual must be notified. This form must be completed and be available to CITB EQA's.

Statements

4. If at any time during the CITB ITC/SSP courses/testing my participation might result in an actual, potential or perceived conflict of interest, I will immediately report the circumstances to the appropriate Authorised Individual.

Declaration Guidance

Declaration A should be signed if there are no actual, potential or perceived conflicts of interest. Sign this part if after KCTL have investigated the situation there are no known conflicts of interest

Declaration B should be signed if there are actual, potential or perceived conflicts of interest. The conflicts of interest and mitigation must be stated below, as must the role that the individual will be carrying out (where appropriate). An Authorised Individual must also sign Declaration B to confirm that they accept that appropriate mitigations have been put in place.

Declaration A (if no conflicts of interest)

By signing this Form, I declare that I have read and accept the Statements above, and that there are no conflicts of interest of any nature which would prevent me from participating in the aforementioned procurement.

If any actual, potential or perceived conflicts of interest arise in the future, I will inform an Authorised Individual immediately.

Name:

Job Title: Organisation / Department:

Signature: Date:

Declaration B (if actual, potential of perceived conflicts of interest)

By signing this Form, I confirm that the conflicts of interest have been mitigated appropriately to allow me to participate in a suitable role.

If any other actual, potential or perceived conflicts of interest arise in the future, I will inform an Authorised Individual immediately.

Name:

Job Title: Organisation / Department:

Signature: Date:

My conflict(s) of interest, including mitigations, is/are:

Conflict of interest *[insert text]*

Mitigation *[insert text]*

[Delete as appropriate]

Therefore my role in the procurement will be *[briefly describe role here]*

OR

Therefore I will not have a role in the procurement.

Authorised Individual

By signing this Form, I confirm that the conflicts of interest have been mitigated appropriately, and therefore the individual's role in the procurement, is appropriate.

Name:

Job Title: Organisation / Department:

Signature: Date:

CITB SSP Examination requirements

1. The examination invigilator is responsible for setting up the room, as detailed below (see paragraph 2) and within your quality management system. The invigilator may ask the delegates to leave the room whilst this is completed.

2. Examination rooms must meet the following requirements, prior to any examination being administered.

- They must be suitably quiet, in an undisturbed location, with adequate space, lighting and ventilation.
- There must be a minimum of 1.25 m between delegates (so they cannot see each other's work).
- There must be a clean desk environment, with no notes, pads, course materials, etc. visible.
- Posters or display materials, which may assist the delegates, must not be visible (except for emergency signage).
- A clock must be visible to all delegates.

3. The final 10/15 minutes of the examination is open book examination (NOT HSA). Therefore, course publications are allowed to be open for this period of the examination only.

4. All telephonic and information technology devices must be switched off prior to the start of the examination. Where a delegate has chosen a downloadable or electronic publication, a hardcopy of the publication must be provided for the examination.

5. If a delegate leaves the examination prior to its conclusion, they will not be permitted to re-enter the examination room until the final delegate has finished and the trainer or invigilator invites the delegate back.

Invigilation requirements

6. All course examinations must be invigilated to prevent collusion between the delegates.

7. Invigilators can be the course trainer and/or another person who is aware of the examination and invigilation process. This person cannot be a delegate of the course.

8. You must ensure that delegates are aware of their responsibilities, as follows.

- They must not communicate with anyone other than the invigilator during the examination.
- To communicate with the invigilator, they must first raise their hand.
- To change any answers, they must cross out their incorrect entry, make a further entry and initial the new answer.
- There must not be any eating, drinking or smoking during the examination.

Examination resits

9. There is an option for an examination to be re-taken (see individual course appendices for details) if the delegate fails on the first attempt.

10. A training provider may wish for an examination resit to be held on the last day of the course. The delegate must agree and be given sufficient time to prepare for this. The examination paper for the resit must not be the same as the first paper taken by the delegate.

11. It is therefore a requirement that the trainer has an alternative examination paper available in the event of this occurrence.

12. Resit results will be confirmed, and details of the resit noted on Part B of the course assessment report.

information taken from the Construction Industry Training Board Quality Assurance Requirements March 1v1.

Special considerations and reasonable adjustments

13. Delegates with special assessment requirements can request the assistance of the invigilator, if

required. Discussions to accommodate delegates with special requirements should be arranged.

prior to the course and separate arrangements must be put in place.

Prior to course commencement, training organisations should identify any special requirements. that delegates may have, such as physical disabilities, including sight, hearing, or writing, and learning or reading difficulties (for example, dyslexia). It is important to remember that sensitive. information about the delegate has been offered voluntarily and it should be respected as confidential and in accordance with data protection and equality legislation.

In circumstances where assistance is required the training organisation should know that under the Equality Act 2010, the training organisation is specifically required to make 'reasonable. adjustments' or give 'special consideration' to enable everyone to have an equal opportunity to complete the course.

You must also be mindful not to make the course easier or for any individual to gain an advantage.

through any special considerations or reasonable adjustments that you apply. The integrity of the examination must not be compromised.

You must discuss with the delegate what support they need and be prepared to arrange for adaptations (for example, the examination can be held in a separate room and questions can be read to the delegate), which may include additional staff support.

CITB Course Materials

A statement is included on the course registers to state that by signing this register they are confirming that correct course materials have been supplied.

CITB Approved Training Organisation Procedures

How to add an achievement in the Construction Training Register

Before you log into the system, you need to have the following pieces of information:

the learner's name.

the learner's unique ID (which could include the Unique Learner Number (ULN),

National Insurance (NI), or Individual ID/Registration number)

the employer's registration number, and the title of the course that the learner has just completed.

Sign into the CITB online services portal (External link - Opens in a new tab or window). You will need the email address you used when you first set up your ATO account and your password.

Once you have logged in, you need to select whether you're adding an individual achievement or bulk achievements.

To add an individual achievement, you first need to search for the learner's record.

Once you have found that record, choose Submit Individual Achievement and fill in the required fields.

To add bulk achievements, make sure that you have read the guidance notes which are linked in the on-screen instructions before you do any bulk upload.

Please use the CSV file template that is provided on the portal to make a bulk upload of achievements - no other file formats will be accepted.

You have 2 days from adding the achievement to make any final changes, before it is submitted for grant payment. You can find these by clicking on the View Achievements tab.

Note from 1st April 2023 the rule for CITB grants have changed to reflect that No Training that does not lead to a CSCS logoed card will be able to claim grant, this means data from KCT registered accrediting bodies (AO's) will no longer be accepted for grant. Data from the AO's cannot be used in future only CPCS & NPORS Construction cards will be accepted for any plant training and grants.

On Training/Testing being booked a CITB information form for ATO purposes must be completed by the customer which must include the following details,

Company Name

Levy Number

GET Code

Date Completed

Course location

See the following form for details.

Confidential CITB ATO Information for Grant Purposes.

Employer						Employer Levy No	
Course						GET CODE	
Location of Training						Date Completed	
First Name	Surname	Email	Tel	DOB	NI Number	CITB No (if known)	Address

KCTL Completed upload of this information on		By KCT Staff Member	
This information will be attached to the course until approved by CITB, once this has been completed this sheet will be destroyed securely. Please make sure candidates are aware of why this information is being requested.			

CITB SSP Procedures

Course Portfolio for KCTL Administration & QA Process

1. Identify dates for training on company calendar.
2. Notify CITB of courses scheduled to be delivered over 3-month period **ssp@citb.co.uk**
3. Notify CITB ref Teams Link for external monitoring.
4. Notify CITB QA if notified courses are cancelled or postponed **ssp@citb.co.uk**
5. Receive enquiry from customer.
6. Inform customer of range of courses offered by KCTL accredited by CITB.
7. Inform customer of prices plus registration per person:

- open courses (available to more than one customer) or
- closed courses (only available to that specific customer).

8. Send course outline Aims and Objectives found in the CITB Site Safety Plus Scheme Rules, including booking form, and requirements including terms and conditions and directions. Emphasise the need to bring Passports and Driving licence to confirm proof of identity.

   Check booking form to ensure all information has been included (Full name, home address, driving licence number, issuing authority).
9. Print power point presentation per learner relevant to the course
10. On the day of the course ensure all delegates have arrived and signed in at reception, and also complete course register including time in and time out.
11. Remind Instructor of need to check all licences and passports against individuals attending and record on Course Register form (see '10' above).
12. Audit feedback evaluation and compare with previous courses.
13. confirmation of attendance for all delegates inputting their details.
14. Print off payment details and store in file.
15. Despatch Certificates.

CITB Instructor Approval

All instructors must have relevant industry experience relating to the subject area delivered. Evidence includes a CV detailing the length of experience in the subject / sector, appropriate teaching/ instructor certificate from an approved accrediting/ awarding body, relevant operating certificates (preferably current within the past 5 years), knowledge of health & safety legislation, and a minimum of a current Emergency First Aid Certificate. Details of at least 2 referees are required one of which should be either previous employer or senior contract manager.

CITB Complaints and appeals procedure.

In the initial instance, complaints and appeals should be directed to the Accredited Training Provider in this case Keith Cook Training Limited. If the complaint or appeal cannot be resolved by the training provider, the dispute should be put in writing to:

Approval and Compliance Manager
CITB Quality Assurance Team
Sand Martin House
Peterborough
PE2 8TY

Use a Defibrillator

What a defibrillator is;

A defibrillator is a piece of equipment that checks someone's heartbeat.

It can also give electric shocks if someone goes into cardiac arrest.

Cardiac arrest is when your heart stops beating so there is no heartbeat.

This means your heart is not pumping blood around the body to important organs like the brain.

The electric shocks can make your heart start to beat again.

Other names for a defibrillator

A defibrillator can also be called an AED or a PAD.

AED stands for Automated External Defibrillator.

PAD stands for Public Access Defibrillator.

A defibrillator, AED and PAD are the same and are used in the same way. In this policy we call it a defibrillator.

When to use a defibrillator

You should use a defibrillator at the same time as CPR.

CPR on an adult and a child training is completed in the Emergency First Aid at Work course which is completed every 3 years.

You should only use a defibrillator if you are with someone else. 1 person needs to keep doing CPR.

When training at a customer's site either confirm the location of their defibrillator or if not onsite call 999 or 112 and to find a defibrillator.

If you are alone, do not worry about the defibrillator. Call 999 or 112 and put them on speakerphone so you can start CPR.

How to use a defibrillator

Turn the defibrillator on and listen to what it tells you to do. 1 person will need to keep doing CPR.

Take all the clothing off the person's chest.

Open the defibrillator. There might be some scissors inside to help you cut off their top and or under garments.

There will be 2 pads that you will need to place on their chest.

The pads will have pictures on them to show you where to put them.

1 pad is put on the right side of their chest, at the top. The other pad goes under their left armpit. The defibrillator will also tell you where to put the 2 pads.

Before you put the pads on their chest, you might need to shave their chest, so the pads stick on properly.

There might be a razor inside the defibrillator. Do not worry if not.

Peel the plastic off each pad and stick them in the right place.

When the pads are on the defibrillator will tell you to stop CPR and it will check their heartbeat.

The defibrillator will tell you if it needs to give the person a shock.

Shout stand clear and make sure no one is touching the person.

You can then press shock on the defibrillator.

The defibrillator will let you know when it is safe to do CPR again.

The defibrillator might need to give another electric shock. You should keep doing CPR until the defibrillator tells you to stop.

Do CPR until a health expert comes or you are too tired to keep going.

If the person starts to breathe normally by themselves, you can put them in the recovery position.

Your Emergency First Aid at Work course informs you on how to put an adult or child in the recovery position.

Do not turn off the defibrillator or take the pads off the person.

CITB Fair Notice Form

Fair Processing Notice for CITB Assured Courses

The information you provide to the CITB Approved Training Organisation, Keith Cook Training Limited, will be used for administering Training Courses and for purposes connected with the Construction Industry Training Board's ("CITB") role as an Industrial Training Board in accordance with the Industrial Training Act 1982.

Your data will be held securely and treated confidentially and will not be disclosed to external parties other than as required for the purposes described above. This may include sharing your information on the CITB Construction Training Register as well as with employers, awarding organisations, competency card schemes or training providers.

Further information, including your legal rights and how your information may be used, can be found by: • viewing the CITB Privacy Notice online at https://www.citb.co.uk/utility links/privacy-policy-cookies/ • asking the Approved Training Organisation for information about how they manage your personal data.

PLEASE COMPLETE THE FOLLOWING IN BLOCK CAPITALS WHERE APPLICABLE

NAME			
Date of Birth			
National Insurance Number			
Email			
Telephone Number			
Full Home Address			
Photo ID TYPE		**Last 4 digits of ID**	
Signature			
All data on this form will be uploaded to CITB for the following assured course			
COURSE TITLE			
GETCODE	**GET0000**	**COURSE END DATE**	
ACCREDITING BODY USED			
EMPLOYER		**CITB LEVY No**	

Keith Cook Training Limited (KCTL) – Fair Processing Notice

Purpose of This Notice
This Fair Processing Notice (also known as a Privacy Notice) outlines how KCTL collects, uses, retains, and shares personal data in a lawful and transparent manner.

Use of Personal Information
We process personal data for the following purposes, including but not limited to:

1. Registering accurate trainee information with awarding bodies.
2. Facilitating access to funding options.
3. Ensuring data is only accessed if publicly available or with consent.
4. Coordinating with relevant organisations to support appropriate training.
5. Enhancing training quality and standards.
6. Planning for future training needs.
7. Conducting audits and quality assurance.
8. Training instructors and assessors.
9. Reporting performance statistics.
10. Monitoring use of public funds.
11. Identifying organisational risks.
12. Strategic training planning.
13. Evaluating policies and procedures.
14. Ensuring safety compliance.

Why We Collect Your Information
Your records support the delivery of effective training by:

- Providing trainers and assessors with accurate information.
- Enabling appropriate training arrangements.
- Supporting continuity of training across staff.
- Investigating concerns or complaints.

Data Confidentiality
All KCTL staff are legally obligated to maintain confidentiality under the common law duty of confidence and the UK Data Protection Act 2018, aligned with GDPR. Only authorised personnel may access or amend your records, and data will not be shared without your consent unless legally required.

Legal Basis for Processing
KCTL may process personal data under lawful bases other than consent, including tasks carried out in the public interest or for compliance with accrediting bodies. Processing is conducted only when necessary, proportionate, and legally justified.

Your Data Rights
Under GDPR, you have the right to:

- Access your personal data via a Subject Access Request (SAR).

- Request rectification of inaccurate or incomplete data.
- Withdraw consent or opt out of data sharing (except where exemptions apply).
- Be informed of how your data is used and protected.
- Lodge complaints with the supervisory authority if your rights are infringed.

Subject Access Requests
To request access to your records, contact:
Information Requests
✉ admin@kcts.me.uk
(Note: Email transmission may not be secure.)

Requests are free of charge unless deemed excessive or repetitive. In such cases, a reasonable fee may apply. Access may be limited if disclosure could cause harm or infringe on another individual's privacy.

Record Amendments
If you believe your data is incorrect, you may request rectification verbally or in writing. We will respond within one calendar month. Requests may be refused if manifestly unfounded or excessive, with justification provided.

Certification Amendments
Re-certification or changes to accreditation documents may incur fees set by the relevant awarding bodies. Please refer to their websites for details.

Would you like this formatted into a downloadable document or tailored for a specific audience (e.g., trainees, staff, partners)?

Your Rights Under GDPR

Under the General Data Protection Regulation (GDPR), you have the following rights:

1. **Right to be informed** – about how your data is collected and used.
2. **Right of access** – to view the personal data we hold about you.
3. **Right to rectification** – to correct inaccurate or incomplete data.
4. **Right to erasure** – to request deletion of your data under certain conditions.
5. **Right to restrict processing** – to limit how your data is used.
6. **Right to data portability** – to obtain and reuse your data across services.
7. **Right to object** – to data processing in specific circumstances.
8. **Rights related to automated decision-making and profiling** – to challenge decisions made without human involvement.

For detailed guidance on these rights, please refer to the Information Commissioner's Office (ICO) website.

Further Information

For questions or concerns regarding how your data is used, please contact the KCTL Admin Team:
✉ **Email:** admin@kcts.me.uk

NEXT REVIEW DATE

02/01/2027

END